DIE UNIVERSELLE ZERFÄLLUNGSALGEBRA EINES NORMIERTEN POLYNOMS

Dissertation
zur Erlangung des Grades eines
Doktors der Naturwissenschaften
dem Fachbereich Mathematik
der Eberhard-Karls-Universität zu Tübingen

vorgelegt von
Eberhard Scherzler
aus Tübingen

1974

74 143

DIE UNIVERSELLE ZERFÄLLUNGSALGEBRA EINES NORMIERTEN POLYNOMS

Dissertation
zur Erlangung des Grades eines
Doktors der Naturwissenschaften
dem Fachbereich Mathematik
der Eberhard-Karls-Universität zu Tübingen

vorgelegt von
Eberhard Scherzler
aus Tübingen

1974

UNIV.
LEIDEN
BIBL.

Tag der mündlichen Prüfung: 5. Februar 1974

Dekan: Professor Dr. H. Heyer

1. Berichterstatter: Professor Dr. G. Michler

2. Berichterstatter: Dozent Dr. C. M. Ringel

INHALTSVERZEICHNIS

Einleitung 1

Bezeichnungen 6

§1 Die universelle Zerfällungsalgebra Z(f,R) eines normierten Polynoms 7

§2 Die S_n-Normalität von Z(f,R) 13

§3 Anwendung der universellen Zerfällungsalgebra bei der Henselisierung 17

§4 Anwendung der universellen Zerfällungsalgebra auf separable Polynome 32

§5 Die Automorphismengruppe von Z(f,R) über einem zusammenhängenden Ring R 36

§6 Die Dimension des Radikals von Z(f,R) über einem Körper R 46

Literaturverzeichnis 54

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41546528_0029

EINLEITUNG

Die universelle Zerfällungsalgebra Z(f,R) eines normierten Polynoms f vom Grad n über dem kommutativen Ring R ist der größte Faktorring des Polynomringes $R[X_1,\ldots,X_n]$, über dem f in Linearfaktoren zerfällt. Sie wurde 1968 von A. Dress [4] eingeführt und in der Theorie der Hensel-Ringe verwendet. Unabhängig davon untersuchte T. Nagahara [14] 1972 diese Algebra und setzte sie in der Theorie der separabeln Polynome ein.

Die vorliegende Arbeit untersucht zuerst Z(f,R), gibt anschließend neue Anwendungen in den beiden erwähnten Gebieten und befaßt sich dann mit der Automorphismengruppe von Z(f,R).

Die beiden ersten Paragraphen sind vorbereitender Art. In §1 wird die universelle Zerfällungsalgebra Z(f,R) eingeführt und eine alternative Konstruktion angegeben, welche unter anderem zeigt, daß Z(f,R) ein freier R-Modul der Dimension n! und ganze Erweiterung von R[X]/(f) ist. Diese Ergebnisse sind auch in [14] bei Nagahara enthalten. §2 weist die für alle folgenden Paragraphen wichtige S_n-Normalität von Z(f,R) nach, deren Bedeutung zuerst von A. Dress [4] erkannt worden ist.

In §3 wenden wir die universelle Zerfällungsalgebra auf das Problem der Henselisierung eines kommutativen

Ringes R nach einem Ideal $\underline{a}$ an. Unter einem Paar $(R,\underline{a})$ verstehen wir hier stets einen kommutativen Ring R mit einem Ideal $\underline{a} \subseteq R$.

Nach S. Greco [7] heißt das Paar $(R',\underline{a}')$ Hensel-Paar, wenn das Henselsche Lemma bezüglich des Ideals $\underline{a}'$ gilt.

Die Henselisierung von $(R,\underline{a})$ ist die Lösung eines universellen Problems: das Hensel-Paar $(\overset{\mathrm{H}}{R},\overset{\mathrm{H}}{\underline{a}})$ mit dem Morphismus $H:(R,\underline{a}) \longrightarrow (\overset{\mathrm{H}}{R},\overset{\mathrm{H}}{\underline{a}})$ heißt Henselisierung von $(R,\underline{a})$, wenn es zu jedem Morphismus φ von $(R,\underline{a})$ in ein Hensel-Paar $(R',\underline{a}')$ genau einen Morphismus ψ von $(\overset{\mathrm{H}}{R},\overset{\mathrm{H}}{\underline{a}})$ in $(R',\underline{a}')$ mit $\psi H = \varphi$ gibt.

Bei der Konstruktion der Henselisierung spielen sowohl in den Beweisen von Nagata [17] als auch später von Greco [7] die Abschwächungen N-Paar und N'-Paar (vgl. Definition 3.2) eine wichtige Rolle. In [7] konstruiert Greco den sogenannten N-Abschluß des Paars $(R,\underline{a})$ als direkten Limes und zeigt dann, daß es sich dabei um die Henselisierung handelt. Die entscheidende Schwierigkeit hierbei ist der auch bei Greco recht umfängliche Beweis, daß Hensel-Paare und N-Paare dasselbe sind ([7, Th. 5.11]).

Lokale Hensel-Paare werden von G. Azumaya in [2] wie folgt charakterisiert: Das Paar $(R,\underline{m})$, wo R ein lokaler kommutativer Ring mit dem maximalen Ideal $\underline{m}$ ist, ist ein Hensel-Paar genau dann, wenn man für jede über R ganze (nicht notwendig kommutative) R-Algebra Z und jedes zweiseitige Ideal $\underline{z}$ von Z Idempotente von $Z/\underline{z}$

nach Z heben kann.

Ziel des §3 ist ein zyklischer Beweis für den folgenden Satz (Greco [7, Th. 5.11] und [5, Th. 3.1])

Satz 3.17

Für das Paar $(R,\underline{a})$ sind äquivalent:

(A) $(R,\underline{a})$ ist ein Hensel-Paar.

(B) $(R,\underline{a})$ ist ein N-Paar.

(C) $(R,\underline{a})$ ist ein N'-Paar.

(D) $\underline{a} \subseteq \mathrm{Rad}(R)$, und für jede R-Algebra C der Form $C = R[X]/(f)$, wo f ein normiertes Polynom $\in R[X]$ ist, kann man Idempotente von $C/\underline{a}C$ nach C heben.

Der gegenüber Greco wesentlich neue Beweisgedanke ist die Verwendung der S_n-Normalität der universellen Zerfällungsalgebra im Sinne von Dress [4]. Außerdem erhalten wir als einfache Folgerung den zitierten Satz von Azumaya (Folgerung 3.18).

In den restlichen Paragraphen dieser Arbeit studieren wir die Ringstruktur von Z(f,R) im Zusammenhang mit den Faktorisierungen des normierten Polynoms f.

§4 enthält den Satz:

Satz 4.7

Das normierte Polynom $f \in R[X]$ ist genau dann separabel, wenn die universelle Zerfällungsalgebra Z(f,R) eine separable R-Algebra im Sinne von Auslander und Goldman [1] ist.

Als Anwendung des Satzes 5.7 zeigen wir in §5 die Folgerung 5.9:

Für einen zusammenhängenden Ring R ist die Gruppe $\mathrm{Aut}_R Z(f,R)$ der Automorphismen der universellen Zerfällungsalgebra $Z(f,R) = Z$ eine zerfallende Erweiterung von $\prod_{i=1}^{k} \mathrm{Aut}_R Ze_i$ durch die symmetrische Gruppe S_k, wobei $1_Z = e_1 + \cdots + e_k$ die Zerlegung des Einselements in primitive orthogonale Idempotente ist. Für die Anzahl k der direkten Summanden Ze_i von Z gilt $k \geqslant n$ oder genau eine der drei Möglichkeiten (a) $k=1$, (b) $k=2$, (c) $k=3$ und $n=4$.
Jeder dieser Fälle kann auftreten, wie die Beispiele am Schluß von §6 zeigen.

Falls R ein kommutativer Körper ist, läßt sich die Struktur von Z(f,R) genauer bestimmen. So können wir in §6 ein notwendiges und hinreichendes Kriterium für die Halbeinfachheit von Z(f,R) angeben.

Satz 6.3

Z(f,R) ist halbeinfach genau dann, wenn gilt:

(i) f(X) ist ein Produkt von paarweise verschiedenen irreduziblen normierten Polynomen $g_i(X) \in R[X]$, welche entweder separabel oder quadratisch-inseparabel sind, und

(ii) der Inseparabilitätsgrad $(K:R)_{ins}$ des Zerfällungskörpers K über R ist 2^r, wo r die Anzahl der quadratisch-inseparabeln Polynome $g_i(X)$ ist.

Wenn char R $\neq 2$ ist, so ist Z(f,R) halbeinfach genau dann, wenn f(X) Produkt von paarweise verschiedenen irreduziblen separablen Polynomen $g_i(X) \in R[X]$ ist, d. h. wenn f(X) separabel ist.
Hierbei benutzen wir die in Lemma 6.2 abgeleitete Formel für die Dimension des Radikals von Z(f,R)

$$\dim_R \mathrm{Rad}(Z(f,R)) = n! - n!\left(\frac{(K:R)_{ins}}{|H|}\right)$$

wobei K der Zerfällungskörper von f, $(K:R)_{ins}$ der Inseparabilitätsgrad von K über R und H eine Untergruppe der symmetrischen Gruppe S_n ist, deren Ordnung sich in Abhängigkeit von der Faktorisierung von f über R bestimmen läßt (vgl. 6.1 und 6.2).
Als Folgerung aus den Ergebnissen von §5 erwähnen wir

Folgerung 6.5

Wenn Z(f,R) halbeinfach ist, gilt für die Ordnung der Galois-Gruppe von K über R $|\mathrm{Gal}(K:R)| = n!/k \cdot 2^r$, wo r die Anzahl der inseparabeln Faktoren in der Primfaktorzerlegung von f ist.

Folgerung 6.7

Sei R ein endlicher Körper und f ein separables Polynom vom Grad $n \geqslant 4$. Die Anzahl k der Blockidempotenten von Z(f,R) ist stets $\geqslant n$.

Herrn Professor Dr. G. Michler bin ich für seine Anregungen und unablässigen Ermunterungen sehr zu Dank verpflichtet.

BEZEICHNUNGEN

Im folgenden sind alle Ringe, Algebren und Körper kommutativ mit Einselement; die einzige Ausnahme von dieser Regel in §3 wird besonders erwähnt.
Moduln sind unitär, Ringhomomorphismen bilden das Einselement auf das Einselement ab. Eine Algebra S über dem Ring R ist ein Ringhomomorphismus $R \longrightarrow S$.
In §3 treten Paare $(R,\underline{a})$ auf; dabei handelt es sich stets um einen kommutativen Ring R mit dem Ideal $\underline{a} \leq R$.
Ein Morphismus $(R,\underline{a}) \longrightarrow (R',\underline{a}')$ ist ein Ringhomomorphismus $\varphi: R \longrightarrow R'$ mit $\varphi^{-1}(\underline{a}') = \underline{a}$.
Rad(R) bezeichnet das Jacobson-Radikal des Ringes R.
Die R-Algebra R' ist ein Erweiterung von R, wenn der Ringhomomorphismus $R \longrightarrow R'$ injektiv ist.

Für die weiteren Bezeichnungen und Definitionen sei auf Lang [12] und für die Gruppentheorie auf B.Huppert: Endliche Gruppen I. (Springer-Verlag Berlin/ Heidelberg/ New York 1967) verwiesen.

§ 1 DIE UNIVERSELLE ZERFÄLLUNGSALGEBRA EINES NORMIERTEN POLYNOMS

Definition 1.1 (Dress[4])
Sei R ein Ring und f ein normiertes Polynom in $R[X]$ vom Grad n, $f = f(X) = X^n - a_1X^{n-1}+-\ldots+(-1)^n a_n$. Mit $s_i = s_i(X_1,\ldots,X_n)$ (für i=1,...,n) bezeichnen wir die elementarsymmetrischen Polynome im Polynomring $R[X_1,\ldots,X_n]$ in den Unbestimmten $X_1,\ldots,X_n$, wobei jeweils s_i homogen vom Grade i ist. $\underline{a}$ sei das von den Elementen $s_i - a_i$ (i=1,...,n) in $R[X_1,\ldots,X_n]$ erzeugte Ideal. Die R-Algebra $Z(f,R) := R[X_1,\ldots,X_n]/\underline{a}$ heißt die universelle Zerfällungsalgebra von f über R.

Z(f,R) wird als R-Algebra von den Elementen $z_i := X_i+\underline{a}$ (i=1,...,n) erzeugt, und das Polynom f^ζ , wo ζ der kanonische Homomorphismus $R \longrightarrow Z(f,R)$ ist, zerfällt über Z(f,R) in Linearfaktoren:

$$\begin{aligned} f^\zeta(X) &= X^n - (a_1 + \underline{a})X^{n-1} +-\ldots+(-1)^n(a_n + \underline{a}) \\ &= X^n - (s_1 + \underline{a})X^{n-1} +-\ldots+(-1)^n(s_n + \underline{a}) \\ &= \prod_{i=1}^{n}(X - (X_i+\underline{a})) \\ &= \prod_{i=1}^{n}(X - z_i). \end{aligned}$$

T.Nagahara verwendet in [14] die Algebra Z(f,R); die Ergebnisse dieses Abschnitts finden sich auch bei ihm.

Zur Rechtfertigung der Bezeichnung "universelle Zerfällungsalgebra" beweisen wir:

Satz 1.2

Wenn B eine R-Algebra ist, über welcher das Polynom f so in Linearfaktoren zerfällt, $f = \prod_{i=1}^{n} (X - w_i)$, daß B von den Wurzeln w_i erzeugt wird, so gibt es genau einen R-Epimorphismus $\varepsilon : Z(f,R) \longrightarrow B$ mit $\varepsilon(z_i) = w_i$ für alle i=1,...,n.

Beweis: Es gibt genau einen R-Epimorphismus $\bar{\varepsilon}$ von $R[X_1,...,X_n]$ auf B mit $\bar{\varepsilon}(X_i) = w_i$ (i=1,...,n). Da $\bar{\varepsilon}(s_i - a_i) = 0$ (Vietasche Wurzelsätze) ist $\ker\bar{\varepsilon} \supseteq \underline{a}$; also gibt es genau einen R-Epimorphismus ε von Z(f,R) auf B mit $\varepsilon(z_i) = w_i$ für alle i=1,...,n.

Folgerung: Z(f,R) ist der größte Faktorring von $R[X_1,...,X_n]$, über dem f in Linearfaktoren zerfällt.

Wir geben jetzt eine andere Konstruktion von Z(f,R).

1.3

Sei R ein Ring und f ein normiertes Polynom in R[X]. Die R-Algebra $R_1 := R[X]/(f)$ ist eine ganze Erweiterung von R. Das Element $u_1 := X+(f)$ erzeugt R_1 als R-Algebra, und $1, u_1, ..., u_1^{n-1}$ ist eine Modulbasis des freien R-Moduls R_1. Außerdem gilt $f(Y) = (Y - u_1)\cdot f_1(Y)$, wo $f_1(Y)$ ein normiertes Polynom vom Grade n-1 in $R_1[Y]$ ist.

Setzt man $R_0 := R$ und $f_0(Y) := f(Y)$, so erhält man in dieser Weise fortfahrend eine Kette von ganzen Erweiterungen

$$R_0 \longrightarrow R_1 \longrightarrow \cdots \longrightarrow R_{n-1} \longrightarrow R_n ,$$

wobei $R_{i+1} = R_i[X]/(f_i)$ gilt, wo f_i ein normiertes Polynom vom Grade n-i in $R_i[X]$ ist, welches $f(X) = \prod_{j=1}^{i} (X - u_j) \cdot f_i(X)$ erfüllt.

R_n wird als R-Algebra von den Elementen u_i (i=1,...,n) erzeugt.

Satz 1.4

Der nach 1.2 eindeutig bestimmte R-Epimorphismus ε von $Z(f,R)$ auf R_n mit $\varepsilon(z_i) = u_i$ (für alle i=1,...,n) ist ein Isomorphismus.

Beweis: Es genügt offenbar zu zeigen, daß es einen R-Algebrenhomomorphismus $\delta : R_n \longrightarrow Z(f,R)$ gibt, welcher u_i auf z_i abbildet. Denn dann ist $\varepsilon\delta = id_{R_n}$ und $\delta\varepsilon = id_{Z(f,R)}$, weil die u_i bzw. z_i die R-Algebra R_n bzw. $Z(f,R)$ erzeugen.

Sei $\delta_0 := \zeta : R \longrightarrow Z(f,R)$ der kanonische Homomorphismus. Hat man nun $\delta_i : R_i \longrightarrow Z(f,R)$ mit $\delta_i(u_j) = z_j$ für j=1,...,i schon konstruiert, dann kann man δ_i wie folgt auf R_{i+1} fortsetzen. Sicherlich existiert ein R-Homomorphismus $\bar{\delta}_{i+1}$ von $R_i[X]$ in $Z(f,R)$, welcher δ_i fortsetzt und X auf z_{i+1} abbildet.

Aus $\prod_{j=1}^{n} (Y - z_j) = f^{\zeta}(Y) = \delta_i(f(Y)) =$

$$= \delta_i\Big(\prod_{j=1}^{i}(Y - u_j)\cdot f_i(Y)\Big) = \prod_{j=1}^{i}(Y - z_j)\cdot\delta_i(f_i(Y))$$

folgt

$\prod_{j=i+1}^{n}(Y - z_j) = \delta_i(f_i(Y))$, weil normierte Polynome keine Nullteiler sind. Folglich ist

$$\bar{\delta}_{i+1}(f_i(X)) = \prod_{j=i+1}^{n}(z_{i+1} - z_j) = 0 .$$

Daher existiert ein R-Homomorphismus $\delta_{i+1}: R_{i+1} \longrightarrow Z(f,R)$ mit $\delta_{i+1}(u_j) = z_j$ für $0 \leq j \leq i+1$.

Man erhält demnach den gesuchten Homomorphismus $\delta = \delta_n$ von R_n auf $Z(f,R)$.

Folgerung 1.5

Die Elemente $\prod_{i=1}^{n} z_i^{m_i}$ mit $0 \leq m_i \leq n-i$ bilden eine Modulbasis des freien R-Moduls $Z(f,R)$, und es ist $\dim_R Z(f,R) = n!$.

Beweis: In 1.3 bilden jeweils die Elemente $u_i^0, u_i^1, \ldots, u_i^{n-i}$ eine Modulbasis von R_i über R_{i-1}. Mit dem Isomorphismus ε aus 1.4 folgt die Behauptung.

Bemerkung 1.6

Mit den Bezeichnungen von 1.3 gilt $Z(f_1,R_1) \cong Z(f,R)$ als R-Algebren, wo $R \longrightarrow R_1$ die R-Algebrenstruktur von $Z(f_1,R_1)$ induziert, denn es ist ja $Z(f,R) \cong R_n = R_1[u_2,\ldots,u_n] \cong Z(f_1,R_1)$.

Lemma 1.7

Die symmetrische Gruppe S_n wirkt auf $Z(f,R)$ durch R-Algebra-Automorphismen (n = Grad von f).

Beweis: Zu jedem π aus S_n gibt es genau einen R-Automorphismus von $R[X_1,\ldots,X_n]$, welcher X_j auf $X_{\pi(j)}$ abbildet. Dieser Automorphismus läßt die Elemente $s_i - a_i$ und somit auch das Ideal $\underline{a}$ fest. Man erhält also einen Automorphismus der R-Algebra $Z(f,R)$, welcher z_j auf $z_{\pi(j)}$ abbildet. Man sieht sofort, daß die beschriebene Abbildung von S_n in $\mathrm{Aut}_R Z(f,R)$ ein Homomorphismus ist.

Bezeichnung: Das Bild von S_n in $\mathrm{Aut}_R Z(f,R)$ unter dem obigen Homomorphismus bezeichnen wir mit $\overline{S}_n$.

Lemma 1.8

Für $n \neq 2$ ist die Abbildung $S_n \longrightarrow \mathrm{Aut}_R Z(f,R)$ ein Monomorphismus.

Beweis: Wenn die Abbildung kein Monomorphismus ist, so ist $n > 1$ und es gibt $\sigma,\tau \in S_n$ und $j \in \{1,\ldots,n\}$ mit $\sigma(j) \neq \tau(j)$ und $\overline{\sigma} = \overline{\tau}$. Folglich gilt $z_{\sigma(j)} = \overline{\sigma}(z_j) = \overline{\tau}(z_j) = z_{\tau(j)}$, und aus der n-fachen Transitivität von S_n folgt für alle $l,m \in \{1,\ldots,n\}$ $z_l = z_m$. Nun ist $R[z_1] \cong R[X]/(f)$ ein freier R-Modul der Dimension n. Weil $z_m = z_1$ für alle $m=1,\ldots,n$ ist, folgt $R[z_1] = R[z_1,\ldots,z_n] = Z(f,R)$. Da aber $Z(f,R)$ nach 1.5 die Dimension $n!$ besitzt, folgt $n = n!$, also $n = 2$.

Bemerkung 1.9

Der Homomorphismus $S_2 \longrightarrow \mathrm{Aut}_R Z(f,R)$ ist genau dann kein Monomorphismus, wenn f die Form $X^2 + a$ hat und in R $1+1=0$ gilt.

Beweis: Wenn in R $1+1=0$ ist und $f = X^2 + a$, so gilt $z_1 - z_2 = z_1 + z_2 = 0$, also $z_1 = z_2$; folglich wird das erzeugende Element von S_2 auf $1 \in \mathrm{Aut}_R Z(f,R)$ abgebildet.

Sei umgekehrt $S_2 \longrightarrow \mathrm{Aut}_R Z(f,R)$ kein Monomorphismus, also $z_1 = z_2$. Aus $f = X^2 - (z_1+z_2)X + z_1 z_2$ und $z_1+z_2 = r \in R$ folgt also $(1+1)z_1 - r = 0$. Nun ist aber nach 1.5 $\{1, z_1\}$ eine Modulbasis von $Z(f,R)$, also $1+1 = 0$ und $r = 0$.

§ 2 DIE S_n-NORMALITÄT VON Z(f,R)

Nach Lemma 1.7 ist Z(f,R) eine (R,S_n)-Algebra im Sinn der folgenden Definition von Dress [4].

Definition 2.1

Sei G eine endliche Gruppe und B eine R-Algebra. G wirke auf B durch durch R-Algebra-Automorphismen. Eine R-Algebra B zusammen mit solch einer Wirkung nennen wir eine (R,G)-Algebra und schreiben die Wirkung von $\gamma \in G$ auf das Element $b \in B$: $b \longmapsto \gamma(b)$.
Seien B,C (R,G)-Algebren und φ ein R-Algebra-Homomorphismus von B in C. Wir nennen φ einen (R,G)-Morphismus, falls φ mit der Wirkung von G vertauschbar ist, d.h. $\varphi(\gamma(b)) = \gamma(\varphi(b))$ für alle $\gamma \in G$ und $b \in B$.

Für die Anwendung von Z(f,R) im nächsten Abschnitt ist die von Dress [4] eingeführte S_n-Normalität von entscheidender Bedeutung. Zu ihrer Formulierung benötigen wir die folgenden Definitionen.

Definition 2.2

Sei $\{X_\gamma : \gamma \in G\}$ eine Menge von Unbestimmten mit der Mächtigkeit von G und V(R,G) der Polynomring über R in den Unbestimmten $(X_\gamma)_{\gamma \in G}$. Wir erklären auf V(R,G) eine Wirkung durch G, indem wir für $\gamma \in G$ festsetzen: für $v \in V(R,G)$ sei $\gamma(v)$ das Bild von v bei dem (eindeutig bestimmten) R-Algebra-Automorphismus von V(R,G), der

X_δ auf $X_{\gamma\delta}$ ($\gamma\delta$ = Produkt von γ und δ in G) für alle $\delta \in G$ abbildet. G wirkt also auf V(R,G) durch Permutieren der Unbestimmten. Offenbar ist V(R,G) mit dieser Wirkung eine (R,G)-Algebra, die universelle (R,G)-Algebra.

Sei B eine (R,G)-Algebra; zu jedem $b \in B$ existiert genau ein (R,G)-Morphismus von V(R,G) in B, der das Element X_ε (ε = Einselement von G) auf b abbildet. Das Bild von $v \in V(R,G)$ unter diesem Morphismus bezeichnen wir mit v(b) ("Einsetzen").
Jede von einem Element erzeugte (R,G)-Algebra ist das Bild von V(R,G) unter dem oben angegebenen Morphismus.

In der klassischen Galoistheorie hat man die folgende Situation: wenn K eine Galoiserweiterung des Körpers k ist und G die Galoisgruppe, dann ist die Menge der unter G invarianten Elemente von K gerade k. Diesen Sachverhalt in geeigneter Form abzuschwächen, ist der Sinn der folgenden Definition.

Definition 2.3

Die (R,G)-Algebra B heißt G-normal, wenn für alle G-invarianten Elemente v von V(R,G) und für alle $b \in B$ die Elemente v(b) in $R.1_B$ liegen.

Die sich anschließenden Folgerungen aus der Definition 2.3 stammen ebenfalls von Dress [4] ,

Folgerung 2.4

Sei B eine G-normale (R,G)-Algebra und $\underline{c}$ ein G-invariantes Ideal in B. Der Faktorring $B/\underline{c}$ ist in kanonischer Weise eine (R,G)-Algebra, welche G-normal ist.

Beweis: Die durch $\gamma(b + \underline{c}) := \gamma(b) + \underline{c}$ auf $B/\underline{c}$ definierte Wirkung ist wegen der G-Invarianz von $\underline{c}$ wohldefiniert und ein Automorphismus der R-Algebra $B/\underline{c}$. Wenn $v \in V(R,G)$ G-invariant ist, dann ist für alle $b \in B$ das Element $v(b)$ in $R \cdot 1_B$, also $v(b + \underline{c}) = v(b) + \underline{c}$ in $R \cdot 1_{B/\underline{c}}$, weil $R \cdot 1_{B/\underline{c}}$ das Bild von $R \cdot 1_B$ beim Epimorphismus von B auf $B/\underline{c}$ ist.

Folgerung 2.5

$Z(f,R)$ ist eine S_n-normale (R,S_n)-Algebra.

Beweis: Mit den Bezeichnungen von 1.1 und 1.7 ist der Ring $B^* := R[X_1,\ldots,X_n]^{S_n}$ der S_n-invarianten Elemente von $B := R[X_1,\ldots,X_n]$ gerade $B^* = R[s_1,\ldots,s_n]$ und B ist eine S_n-normale (B^*,S_n)-Algebra. Nun ist das Ideal $\underline{a}$ von B S_n-invariant, so daß nach 2.4 $Z(f,R) = B/\underline{a}$ eine S_n-normale (B^*,S_n)-Algebra ist. Wegen $B^* \cdot 1_{B/\underline{a}} \cong B^*/\underline{a} \cap B^* \cong R$ ist nun $Z(f,R)$ trivialerweise auch S_n-normale (R,S_n)-Algebra.

Satz 2.6

Die (R,G)-Algebra B ist genau dann G-normal, wenn für alle $b \in B$ und für alle Untergruppen U von G das Element

$$\sum_{\gamma \in G/U} \gamma\Big(\prod_{\beta \in U} \beta(b)\Big),$$

wo G/U ein Vertretersystem von Linksnebenklassen ist, in $R \cdot 1_B$ liegt.

Beweis: vgl. Dress [4, (4)] .

Satz 2.7

Jede G-normale (R,G)-Algebra B ist ganz über R.

Beweis: Jedes Element $b \in B$ erfüllt ein normiertes Polynom mit Koeffizienten aus $R \cdot 1_B$. Die Koeffizienten des Polynoms $\prod_{\gamma \in G}(Y - X_\gamma)$ aus $V(R,G)[Y]$ sind G-invariant; daher ist das normierte Polynom $\prod_{\gamma \in G}(Y - \gamma(b))$ mit der Wurzel b in $R \cdot 1_B[Y]$.

§ 3 ANWENDUNG DER UNIVERSELLEN ZERFÄLLUNGS-ALGEBRA Z(f,R) BEI DER HENSELISIERUNG

In Anlehnung an S.Greco [7] verstehen wir in diesem Abschnitt unter (R,a) stets das Paar bestehend aus dem Ring R und dem Ideal $a \subseteq R$. Der Vereinfachung der Ausdrucksweise dient auch die folgende Definition.

Definition 3.1

Das Paar (R,a) heißt HI-Paar (Heben von Idempotenten), wenn man Idempotente von R/a nach R heben kann, d.h., wenn es zu jedem Idempotent $\bar{e}$ von R/a ein Idempotent e in R gibt, dessen Bild unter dem kanonischen Epimorphismus von R auf R/a gerade $\bar{e}$ ist.
Gibt es zu jedem Idempotent $\bar{e}$ von R/a genau ein Idempotent e von R, dessen Bild $\bar{e}$ ist, so heißt (R,a) ein EHI-Paar (Eindeutiges Heben von Idempotenten).

Definition 3.2 (Greco [7])

Ein normiertes Polynom $f = X^n + r_1X^{n-1} + \cdots + r_n$ in R[X] heißt

N'-Polynom über (R,a), wenn $n \geq 2$, $r_i \in a$ für $i \geq 2$ und r_1 modulo a eine Einheit ist.

N-Polynom über (R,a), wenn $n \geq 2$, $r_n \in a$ und r_{n-1} modulo a eine Einheit ist.

Hensel-Polynom über $(R,\underline{a})$, wenn es folgende Bedingung erfüllt (Hensels Lemma): Ist $\overline{f} = \overline{g}_1\overline{g}_2$ mit zwei relativ primen normierten Polynomen $\overline{g}_i$ aus $(R/\underline{a})[X]$, so existieren zwei normierte Polynome h_1 und h_2 in $R[X]$ mit $f = h_1h_2$, deren Bilder bei dem kanonischen Epimorphismus $R[X] \longrightarrow (R/\underline{a})[X]$ die Polynome $\overline{g}_1$ bzw. $\overline{g}_2$ sind.

Wenn $\underline{a} \subsetneq \mathrm{Rad}(R)$, dann nennen wir das Paar $(R,\underline{a})$ ein

N'-Paar , falls jedes N'-Polynom über $(R,\underline{a})$ eine Wurzel besitzt, die modulo $\underline{a}$ eine Einheit in R ist.

N-Paar , falls jedes N-Polynom über $(R,\underline{a})$ eine Wurzel in $\underline{a}$ besitzt.

Hensel-Paar , falls jedes normierte Polynom aus $R[X]$ ein Hensel-Polynom über $(R,\underline{a})$ ist.

Den Beweisen der Sätze 3.13 und 3.17 stellen wir die folgenden einfachen Hilfssätze voraus (vgl. Greco[7])

Lemma 3.3

Jedes N'-Paar ist ein EHI-Paar.

Beweis: Sei $(R,\underline{a})$ ein N'-Paar und z aus R mit $z^2 - z$ in $\underline{a}$. Das Polynom $f = X^2 + X(2z - 1) + (z^2 - z)$ ist ein N'-Polynom über $(R,\underline{a})$, denn $2z-1 = z+(z-1)$ ist

Einheit in R, weil $z(z-1)$ in Rad(R) ist. f hat also eine Wurzel, welche in R invertierbar ist; die andere Wurzel liegt dann in a. Wenn w diese Wurzel ist, so gilt also $0 = w^2 + w(2z-1) + (z^2-z) = (z+w)^2 - (z+w)$ und $z+w$ ist das gesuchte Idempotent in R. Die Eindeutigkeit ergibt sich aus dem folgenden Lemma.

Lemma 3.4

Wenn $a \subseteq \mathrm{Rad}(R)$ und e,e' Idempotente in R sind, so folgt aus $e \equiv e'$ modulo a, daß e=e' ist.

Beweis: durch einfache Rechnung.

Lemma 3.5

Jedes epimorphe Bild eines N'-Paares ist ein N'-Paar.

Beweis: durch einfache Rechnung.

Lemma 3.6

Jedes Hensel-Paar ist ein N-Paar.

Beweis: durch einfache Rechnung.

Lemma 3.7

Jedes N-Paar ist ein N'-Paar.

Beweis: Sei $f(X) = X^n + d_1X^{n-1} + \cdots + d_n$ ein N'-Polynom über (R,a). Setzt man X=U+V (mit zwei Unbestimmten U und V) und ordnet f(U+V) nach Potenzen von U, so erhält man bekanntlich

$$f(U+V) = U^n + \cdots + f'(V)\cdot U + f(V),$$

wobei $f'(V)$ das aus $f(V)$ durch Ableitung entstehende Polynom ist. Setzt man nun für V den Wert $-d_1$ ein, so gilt $f(-d_1) \in \underline{a}$ und $f'(-d_1)-(-d_1)^{n-1} \in \underline{a}$, denn es ist

$$f(-d_1) \equiv (-d_1)^n + d_1\cdot(-d_1)^{n-1} = 0 \text{ modulo } \underline{a} \text{ und}$$

$$f'(-d_1) \equiv n(-d_1)^{n-1} + (n-1)d_1(-d_1)^{n-2} = (-d_1)^{n-1}$$

modulo $\underline{a}$.

Das Polynom $f(U-d_1)$ aus $R[U]$ ist daher ein N-Polynom über $(R,\underline{a})$ und hat demnach eine Wurzel $a \in \underline{a}$. Folglich hat das Polynom $f(X) \in R[X]$ die Wurzel $a-d_1$, welche modulo $\underline{a}$ eine Einheit ist.

Lemma 3.8

Sei B eine G-normale (R,G)-Algebra und $\underline{c}$ ein G-invariantes Ideal von B. Wenn $(B,\underline{c})$ ein EHI-Paar ist, so ist auch $(R\cdot 1_B, \underline{c}\cap R\cdot 1_B)$ ein EHI-Paar.

Beweis: Sei $\bar{e}$ ein Idempotent in $R\cdot 1_B/\underline{c}\cap R\cdot 1_B$. Wegen $R\cdot 1_B/\underline{c}\cap R\cdot 1_B \subseteq B/\underline{c}$ gibt es nach Voraussetzung in B ein eindeutig bestimmtes Idempotent e, welches $e+\underline{c} = \bar{e}$ erfüllt. Sei $e^* := \prod_{\gamma\in G} \gamma(e)$; sicherlich ist e^* ein Idempotent in B, welches wegen der G-Normalität von B in $R\cdot 1_B$ liegt. Es gilt außerdem $e^* + \underline{c} = \prod_{\gamma\in G} \gamma(e) + \underline{c} = \prod_{\gamma\in G} \gamma(e+\underline{c}) = \prod_{\gamma\in G} \gamma(\bar{e}) = \bar{e}$, da $\bar{e}$ aus $R\cdot 1_{B/\underline{c}}$ und somit invariant unter allen $\gamma\in G$ ist. Es gilt also $e=e^*$ und $(R\cdot 1_B, \underline{c}\cap R\cdot 1_B)$ ist ein EHI-Paar.

Das folgende Lemma ist das Kernstück im Beweis zu Satz 3.13; die G-Normalität der Algebra B wird entscheidend

verwendet.

Lemma 3.9

Sei B eine G-normale (R,G)-Algebra, $\underline{c}$ ein G-invariantes Ideal von B, das in Rad(B) enthalten ist, C die (R,G)-Algebra $B/\underline{c}$ und c_1 ein Idempotent in C, das die Bedingung

(*) für alle γ', γ'' aus G gilt:

$$\gamma'(c_1) \neq \gamma''(c_1) \Rightarrow \gamma'(c_1) \cdot \gamma''(c_1) = 0$$

erfüllt.

Wenn $(R \cdot 1_B, R \cdot 1_B \cap \underline{c})$ ein N'-Paar ist, dann existiert in B ein Idempotent b_1 mit $b_1 + \underline{c} = c_1$.

Beweis: Sei $D := \{\delta \in G : \delta(c_1) = c_1\}$ der Stabilisator von c_1 und $\gamma_1, \ldots, \gamma_k$ ein Repräsentantensystem der Linksnebenklassen von D in G (Bezeichnung: G/D) mit $\gamma_1 = 1_G$. Für $i=1,\ldots,k$ setzen wir $c_i := \gamma_i(c_1)$. Dann ist für $i \neq j$ offenbar $c_i \cdot c_j = 0$, und die c_i sind Idempotente in C.

Sei $\overline{b} \in B$ mit $\overline{b} + \underline{c} = c_1$ und $\overline{b}_i := \prod_{\delta \in D} \gamma_i \delta(\overline{b})$ für alle $i=1,\ldots,k$. Man hat dann

$$\overline{b}_i + \underline{c} = \prod_{\delta \in D} \gamma_i \delta(\overline{b}) + \underline{c} = \prod_{\delta \in D} \gamma_i \delta(\overline{b} + \underline{c}) = \prod_{\delta \in D} \gamma_i \delta(c_1) = c_i$$

und die Koeffizienten des Polynoms

$$f(X) = \prod_{i=1}^{k} (X - \overline{b}_i)$$

liegen in $R \cdot 1_B$, weil das Polynom

$$\prod_{i=1}^{k} (X - \prod_{\delta \in D} X_{\gamma_i \delta}) \quad \text{in } V(R,G)[X] \text{ liegt}$$

und G-invariante Koeffizienten hat. Insbesondere ist dann $\bar{b}_1 + \cdots + \bar{b}_k$ in $R\cdot 1_B$, also $c_1 + \cdots + c_k$ in $R\cdot 1_C$. Die c_i sind paarweise orthogonale Idempotente; daher ist $c := c_1 + \cdots + c_k$ ein Idempotent in $R\cdot 1_C$. Wir behandeln zuerst den Fall $c = 1_C$ und führen dann den allgemeinen Fall darauf zurück.

Sei also zunächst $c = 1_C$. $f(X)$ ist ein N'-Polynom über $(R\cdot 1_B, \underline{c} \cap R\cdot 1_B)$, denn wenn man

$$f(X) = X^k - s_1 X^{k-1} + - \cdots + (-1)^k s_k$$

schreibt (die s_i sind hier die symmetrischen Polynome in den Wurzeln $\bar{b}_j$), so ist $(s_1 - 1_B)$ in $\underline{c}$ wegen $s_1 = \bar{b}_1 + \cdots + \bar{b}_k \equiv 1_B$ modulo $\underline{c}$, und für $i > 1$ sind die Elemente s_i im Ideal $\underline{c}$, weil ja $\bar{b}_m \cdot \bar{b}_n \in \underline{c}$ für $m \neq n$ ist. Nach Voraussetzung besitzt nun $f(X)$ eine Wurzel w in $R\cdot 1_B$, die wegen $R\cdot 1_B \cap \underline{c} \subseteq \mathrm{Rad}(R\cdot 1_B)$ eine Einheit in $R\cdot 1_B$ ist. Sei v das Inverse von w und $P := 1_B - v\bar{b}_1$ und $Q := \prod_{2 \leq i \leq k} (1_B - v\bar{b}_i)$. Dann ist $P\cdot Q = v^k \cdot f(w) = 0$, und man hat

$$P+Q \equiv (1_B - v\bar{b}_1) + (1_B - v(\bar{b}_2 + \cdots + \bar{b}_k)) = 1_B + 1_B - vs_1$$

modulo $\underline{c}$.

Aus $s_i \in \underline{c}$ für $i > 1$ und $f(w) = w^k - s_1 w^{k-1} + \cdots + (-1)^k s_k = 0$ folgt $(w^k - s_1 w^{k-1}) \in \underline{c}$ und daher $(1_B - vs_1) \in \underline{c}$.

Folglich hat man $P+Q \equiv 1_B$ modulo $\underline{c}$, und $P+Q$ ist eine Einheit in B wegen $\underline{c} \subseteq \mathrm{Rad}(B)$.

Also existiert $d \in B$ mit $dP + dQ = 1_B$, und die Elemente dP, dQ sind orthogonale Idempotente in B.

Wegen $d - 1_B = d(1_B - (P+Q))$ und $(1_B - (P+Q)) \in \underline{c}$ ist

$d - 1_B$ in $\underline{c}$, also $dP \equiv P \equiv 1_B - v\overline{b}_1$ modulo $\underline{c}$. Nun ist $1_B - s_1$ und $1_B - vs_1$ in $\underline{c}$ und deshalb $1_B - vs_1 - v(1_B - s_1) = 1_B - v$ in $\underline{c}$; also ist auch $\overline{b}_1 \equiv v\overline{b}_1$ modulo $\underline{c}$, woraus man schließlich $dQ = 1_B - dP \equiv 1_B - P = v\overline{b}_1 \equiv \overline{b}_1$ modulo $\underline{c}$ erhält. $b_1 := dQ$ ist das gesuchte Idempotent.

Sei nun c ein beliebiges Idempotent in $R \cdot 1_C$.
Wegen $R \cdot 1_C = R \cdot 1_B / \underline{c} \cap R \cdot 1_B$ und weil $(R \cdot 1_B / \underline{c} \cap R \cdot 1_B)$ ein N'-Paar ist, läßt sich c zu einem Idempotent b in $R \cdot 1_B$ heben (Lemma 3.3). Wir setzen $B' := Bb$, $B'' := B(1_B - b)$, $\underline{c}' := \underline{c}b$, $\underline{c}'' := \underline{c}(1_B - b)$ und erhalten mit den Bezeichnungen $C' := Cc$ und $C'' := C(1_C - c)$

$$B'/\underline{c}' = C' \quad \text{und} \quad B''/\underline{c}'' = C''.$$

Nach Lemma 2.4 ist B' eine G-normale (R,G)-Algebra. $\underline{c}'$ ist ein Ideal in B', das offensichtlich in Rad(B') enthalten und G-invariant ist. Wegen $c \cdot c_1 = c_1$ ist c_1 in C' und deshalb ein Idempotent, das die Bedingung (*) erfüllt.
Es ist $1_{B'} = 1_B \cdot b = b$ und $1_{C'} = 1_C \cdot c = c$; daher ist $R \cdot 1_{B'} = R \cdot 1_B \cdot b = R \cdot 1_B / R \cdot 1_B (1_B - b)$ und $R \cdot 1_{B'} \cap \underline{c}' = R \cdot 1_B \cdot b \cap \underline{c} \cdot b = (R \cdot 1_B \cap \underline{c}) / ((R \cdot 1_B \cap \underline{c}) \cdot (1_B - b))$ und deshalb $(R \cdot 1_{B'}, \underline{c}' \cap R \cdot 1_{B'})$ als epimorphes Bild von $(R \cdot 1_B, \underline{c} \cap R \cdot 1_B)$ ein N'-Paar nach Lemma 3.5.
Nun ist $c = 1_{C'}$ und es liegt die Situation des oben behandelten Falles vor, für den die Behauptung schon bewiesen ist. Folglich existiert in B' ein Idempotent b_1 mit $b_1 + \underline{c}' = c_1$. Wegen $B' \subseteq B$ ist $b_1 \in B$ und $b_1 + \underline{c} = c_1$.

Wir werden uns jetzt von der einschränkenden Bedingung (*) in Lemma 3.9 befreien. Dazu benötigen wir die folgenden Lemmata über Idempotente.

Lemma 3.10

Sei k eine natürliche Zahl und $K := \{1,\ldots,k\}$. Im Polynomring $\mathbb{Z}[X_1,\ldots,X_k]$ in k Unbestimmten definieren wir für jede Teilmenge T von K die Polynome

$$P_T(X_1,\ldots,X_k) := \prod_{n \in K-T} X_n \qquad \text{und}$$

$$Q_T(X_1,\ldots,X_k) := P_T(X_1,\ldots,X_k) \cdot \prod_{n \in T} (1 - X_n) .$$

Wenn $c_1,\ldots,c_k$ Idempotente aus einem Ring R sind, dann ist für alle $T \subseteq K$ $Q_T(c_1,\ldots,c_k)$ ein Idempotent in R und es gilt für alle $T,S \subseteq K$:

$$S \neq T \implies Q_T(c_1,\ldots,c_k) \cdot Q_S(c_1,\ldots,c_k) = 0.$$

Beweis: durch einfache Rechnung.

Lemma 3.11

Sei $K := \{1,\ldots,k\}$ und $Y = (Y_T)_{T \subseteq K}$ eine Familie von 2^k algebraisch unabhängigen Unbestimmten. Sei $\mathbb{Z}[Y]$ der Polynomring über $\mathbb{Z}$ in diesen Unbestimmten; wir setzen

$$W_\emptyset(Y) := Y_\emptyset \qquad \in \mathbb{Z}[Y]$$

und definieren für jedes $T \subseteq K$ rekursiv das Polynom

$$W_T(Y) := Y_T + \left(1 - \prod_{t \in T} (1 - W_{T-\{t\}}(Y))\right) \in \mathbb{Z}[Y]$$

Es gilt:

(A) Für jedes $T \subseteq K$ ist $W_T(Y)$ ein Polynom $\in \mathbb{Z}[Y]$ in den Unbestimmten Y_S mit $S \subseteq T$ ohne konstanten Term.

(B) Wenn $\hat{b} = (\hat{b}_T)_{T \subseteq K}$ eine Familie von Idempotenten mit der Eigenschaft $T' \neq T'' \Longrightarrow \hat{b}_{T'} \cdot \hat{b}_{T''} = 0$ (für alle $T', T'' \subseteq K$) ist, und wenn man die Elemente $\hat{b}_T$ für die Unbestimmten Y_T einsetzt, dann gilt für jedes $T \subseteq K$: $W_T(\hat{b})$ ist ein Idempotent.

(C) Mit den Bezeichnungen von Lemma 3.10 gilt: Substituiert man die Familie $Q = (Q_T(c_1,\ldots,c_k))_{T \subseteq K}$ für die Familie Y, d.h. setzt man die Elemente $Q_T(c_1,\ldots,c_k)$ für die Unbestimmten Y_T ein, so gilt für alle $T \subseteq K$ $W_T(Q) = P_T(c_1,\ldots,c_k)$.

Beweis: (A) folgt sofort aus der Rekursionsformel mittels vollständiger Induktion nach der Mächtigkeit von T. Unter Verwendung von (A) zeigt man, daß für alle $T \subseteq K$ und alle $t \in T$ $\hat{b}_T \cdot W_{T-\{t\}}(\hat{b}) = 0$ gilt. Folglich ist auch $\hat{b}_T \cdot \left(1 - \prod_{t \in T}(1 - W_{T-\{t\}}(\hat{b}))\right) = 0$. Offenbar ist für jede Teilmenge $T \subseteq K$ und jedes $t \in T$ das Element $(1 - W_{T-\{t\}}(\hat{b}))$ ein Idempotent, also ist auch

$$1 - \prod_{t \in T}(1 - W_{T-\{t\}}(\hat{b}))$$

ein Idempotent. Als Summe zweier orthogonaler Idempotenter ist nun auch $W_T(\hat{b})$ idempotent.

Schreibt man zur Abkürzung Q_T bzw. P_T für die Elemente $Q_T(c_1,\ldots,c_k)$ bzw. $P_T(c_1,\ldots,c_k)$, dann folgt die Gültigkeit von (C) aus der kurzen Rechnung:

$$W_T(Q) = Q_T + \left(1 - \prod_{t \in T}(1 - P_{T-\{t\}})\right) =$$

(wo wir induktiv $W_{T-\{t\}}(Q) = P_{T-\{t\}}$ voraussetzen)

$$= Q_T + 1 - (1 - \sum_{t \in T} P_{T-\{t\}} + \sum_{\substack{\{s,t\} \subseteq T \\ s \neq t}} P_{T-\{s,t\}} - \cdots + (-1)^n P_\emptyset)$$

(wo n die Mächtigkeit von T ist)

$$= Q_T + P_T - (P_T - \sum_{t \in T} P_{T-\{t\}} + \sum_{\substack{\{s,t\} \subseteq T \\ s \neq t}} P_{T-\{s,t\}} - \cdots + (-1)^n P_\emptyset)$$

Der rechts stehende Klammerausdruck ist

$$P_T - \sum_{t \in T} P_T \cdot c_t + \sum_{\substack{\{s,t\} \subseteq T \\ s \neq t}} P_T \cdot c_s \cdot c_t - + \cdots + (-1)^n P_T \cdot \prod_{t \in T} c_t$$

$= P_T \cdot \prod_{t \in T} (1 - c_t) = Q_T$, so daß man schließlich erhält: $W_T(Q) = Q_T + P_T - Q_T = P_T$.

Lemma 3.12

Sei $f: B \longrightarrow C$ ein Epimorphismus der Ringe B und C, seien $c_1, \ldots, c_k$ Idempotente in C. In B existiere eine Familie $\tilde{b} = (\tilde{b}_T)_{T \subseteq K}$ von Idempotenten mit $f(\tilde{b}_T) = Q_T(c_1, \ldots, c_k)$ (Bezeichnungen wie in Lemma 3.10). Dann gibt es in B ein Idempotent b_1 mit $f(b_1) = c_1$.

Beweis: Es gibt in B eine Familie $\hat{b} = (\hat{b}_T)_{T \subseteq K}$ von Idempotenten mit $f(\hat{b}_T) = f(\tilde{b}_T) = Q_T(c_1, \ldots, c_k)$ und der Eigenschaft $T' \neq T'' \Longrightarrow b_{T'} \cdot b_{T''} = 0$ (für alle $T', T'' \subseteq K$). Es genügt nämlich,

$$\hat{b}_T := \tilde{b}_T \cdot \prod_{\substack{S \subseteq K \\ S \neq T}} (1 - \tilde{b}_S)$$

zu setzen. Für $T' \neq T''$ sind $\hat{b}_{T'}$ und $\hat{b}_{T''}$ orthogonal; wegen Lemma 3.10 haben $\hat{b}_T$ und $\tilde{b}_T$ dasselbe Bild unter f.

Auf die Familie $(\hat{b}_T)_{T \subseteq K} =: \hat{b}$ kann man Lemma 3.11 anwenden. Mit $S := \{2,\ldots,k\}$ folgt nach (B), daß das Element $b_1 := W_S(\hat{b})$ ein Idempotent in B ist. Aus (C) erhält man $f(b_1) = W_S(f(\hat{b})) = W_S((f(\hat{b}_T))_{T \subseteq K}) = W_S((Q_T(c_1,\ldots,c_k))_{T \subseteq K}) = W_S(Q) = P_S(c_1,\ldots,c_k) = c_1$.

3.9 bis 3.12 fassen wir im folgenden Satz zusammen.

Satz 3.13

Sei $(R,\underline{a})$ ein N'-Paar und B eine G-normale (R,G)-Algebra. Wenn $\underline{a}B \cap R \cdot 1_B = \underline{a} \cdot 1_B$ ist, so ist $(B,\underline{a}B)$ ein EHI-Paar.

Beweis: Sei c_1 ein Idempotent in $B/\underline{a}B$; wir zeigen zuerst, daß man c_1 zu einem Idempotent b_1 von B heben kann. Sei $D := \{\delta \in G : \delta(c_1) = c_1\}$ und $\gamma_1,\ldots,\gamma_k$ ein Repräsentantensystem der Linksnebenklassen von D in G; es sei $\gamma_1 = 1_G$ und $c_i := \gamma_i(c_1)$ für alle i aus $K := \{1,\ldots,k\}$. Mit den Bezeichnungen von Lemma 3.10 definieren wir für jede Teilmenge $T \subseteq K$ das Idempotent $q_T := Q_T(c_1,\ldots,c_k)$ aus $B/\underline{a}B$. Diese Idempotenten erfüllen die Bedingung (*) in Lemma 3.9; sind nämlich $\gamma',\gamma'' \in G$, so gilt für geeignete Teilmengen T',T'' von K die Beziehung $\gamma'(q_T) = q_{T'}$ und $\gamma''(q_T) = q_{T''}$ und deshalb ist nach Lemma 3.10 die Bedingung (*) erfüllt. Nach Lemma 3.9 kann man also die Familie $q = (q_T)_{T \subseteq K}$ zu einer Familie $\tilde{b} = (\tilde{b}_T)_{T \subseteq K}$ von Idempotenten in B heben; es ist nämlich $\underline{a}B$ ein G-invariantes Ideal von B,

welches in Rad(B) enthalten ist, da B nach 2.7 ganz über $R\cdot 1_B$ ist. Nach Lemma 3.5 ist $(R\cdot 1_B, \underline{a}B \cap R\cdot 1_B) = (R\cdot 1_B, \underline{a}\cdot 1_B)$ ein N'-Paar, so daß die Voraussetzungen von Lemma 3.9 erfüllt sind.
Nun kann man Lemma 3.12 anwenden (wobei f der kanonische Epimorphismus von B auf $B/\underline{a}B$ ist) und erhält ein Idempotent $b_1 \in B$ mit $b_1 + \underline{a} = c_1$. Damit ist bewiesen, daß $(B,\underline{a}B)$ ein HI-Paar ist.
Die Eindeutigkeit beim Heben folgt aus Lemma 3.4 wegen $\underline{a}B \subseteq \mathrm{Rad}(B)$.

Wir ziehen jetzt die zum Beweis des Satzes 3.17 entscheidenden Folgerungen.

Folgerung 3.14

Sei $(R,\underline{a})$ ein N'-Paar und $Z:=Z(f,R)$ die universelle Zerfällungsalgebra des normierten Polynoms f. Das Paar $(Z,\underline{a}Z)$ ist ein EHI-Paar.

Beweis: Aus 1.3 bis 1.5 folgt, daß $R\cdot 1_Z$ direkter Summand in Z und kanonisch isomorph zu R ist. Es ist also $\underline{a}\cdot 1_Z = \underline{a}Z \cap R\cdot 1_Z = \underline{a}$; die Behauptung folgt aus 3.13 und 2.5.

Folgerung 3.15

Sei $(R,\underline{a})$ ein N'-Paar und f ein normiertes Polynom in $R[X]$; sei C die R-Algebra $R[X]/(f)$. Das Paar $(C,\underline{a}C)$ ist ein EHI-Paar.

Beweis: Nach 1.4 und Bemerkung 1.6 gilt für das Polynom

f_1 aus $C[X]$, wo $C := R[X]/(f) \cong R[z_1]$ und $f = (X-z_1)\cdot f_1$ mit $z_1 \in Z(f,R)$ (vgl. 1.1) ist, $Z(f_1,C) \cong Z(f,R)$. Nach 3.14 ist $(Z(f_1,C),\underline{a}Z(f_1,C))$ ein EHI-Paar, also ist nach 3.8 wegen $\underline{a}Z(f_1,C) \cap C = \underline{a}C$ das Paar $(C,\underline{a}C)$ ein EHI-Paar.

Das folgende Lemma stammt von Azumaya [2, 5., Lemma 3] und wurde von Greco in [5] verallgemeinert.

Lemma 3.16

Sei $\underline{a}$ ein Ideal im Ring R, das in Rad(R) enthalten ist, f ein normiertes Polynom in $R[X]$ und C die R-Algebra $R[X]/(f)$. Wenn $(C,\underline{a}C)$ ein HI-Paar ist, dann ist f ein Hensel-Polynom über $(R,\underline{a})$.

Beweis: vgl Greco [5, Lemma 3.2, Proof of Theorem 3.1].

Wir formulieren jetzt das Hauptergebnis dieses Abschnitts.

Satz 3.17

Für das Paar $(R,\underline{a})$ sind äquivalent:

(A) $(R,\underline{a})$ ist ein Hensel-Paar.

(B) $(R,\underline{a})$ ist ein N-Paar.

(C) $(R,\underline{a})$ ist ein N'-Paar.

(D) $\underline{a} \subseteq \mathrm{Rad}(R)$, und für jede R-Algebra C der Form $C = R[X]/(f)$, wo f ein normiertes Polynom $\in R[X]$ ist, ist $(C,\underline{a}C)$ ein EHI-Paar.

Beweis: "(A) $\Longrightarrow$ (B)" Lemma 3.6

"(B) $\Longrightarrow$ (C)" Lemma 3.7

"(C) $\Longrightarrow$ (D)" Folgerung 3.15

"(D) $\Longrightarrow$ (A)" Lemma 3.16

Folgerung 3.18 (Azumaya [2, 5., Theorem 22])
Sei R ein lokaler Ring mit dem maximalen Ideal $\underline{m}$. Das Paar $(R,\underline{m})$ ist ein Hensel-Paar dann und nur dann, wenn für jede über R ganze -nicht notwendig kommutative - R-Algebra Z und jedes zweiseitige Ideal $\underline{z}$ in Z das Paar $(Z,\underline{z})$ ein HI-Paar ist.

Beweis: Die Behauptung folgt aus der Äquivalenz (A)$\Leftrightarrow$(D) in Satz 3.17 und der Äquivalenz (A)$\Leftrightarrow$(C) des folgenden Lemmas.

Lemma 3.19
Sei R ein lokaler Ring mit dem maximalen Ideal $\underline{m}$.
Äquivalent sind:

(A) Für jede R-Algebra C der Form $C = R[X]/(f)$, wo f ein normiertes Polynom $\in R[X]$ ist, ist $(C,\underline{m}C)$ ein HI-Paar.

(B) Für jede R-Algebra der Form $C = R[X]/(f)$, wo f ein normiertes Polynom $\in R[X]$ ist, und für jedes Ideal $\underline{c}$ in C ist $(C,\underline{c})$ ein HI-Paar.

(C) Für jede über R ganze - nicht notwendig kommutative - R-Algebra Z und jedes zweiseitige Ideal $\underline{z}$ in Z ist $(Z,\underline{z})$ ein HI-Paar.

Beweis: (A) $\Rightarrow$(B). Mit der Bezeichnung $C' := C/\underline{c}$ hat man das kommutative Diagramm

$$\begin{array}{ccc} C & \longrightarrow & C' \\ \downarrow & & \downarrow \\ C/\underline{m}C & \longrightarrow & C'/\underline{m}C' \end{array}$$

Wir zeigen, daß man Idempotente von C' nach C heben kann. Sei e' ein Idempotent in C' und $\bar{e}'$ sein Bild in $C'/\underline{m}C'$. Man kann $\bar{e}'$ zu einem Idempotent $\bar{e}$ von $C/\underline{m}C$ heben, denn $C/\underline{m}C$ ist ein Artin-Ring als endlichdimensionaler Vektorraum über dem Körper $R/\underline{m}$ und in (kommutativen) Artin-Ringen kann man Idempotente modulo jedem Ideal eindeutig heben. Nach Voraussetzung kann man nun $\bar{e}$ zu einem Idempotent d von C heben. Sei d' das Bild von d in C'; wir zeigen $d' = e'$. Nach Lemma 3.4 genügt der Nachweis $d' \equiv e'$ modulo $\underline{m}C'$ und $\underline{m}C' \subseteq \mathrm{Rad}(C')$. Ersteres folgt aus der Kommutativität des obigen Diagramms und letzteres aus der Ganzheit von C' über $R \cdot 1_{C'}$.

(B) $\Rightarrow$(C). Sei $e+\underline{z}$ ein Idempotent in $Z/\underline{z}$ und f ein normiertes Polynom in $R[X]$, welches die Nullstelle e hat (Ganzheit von Z) und minimalen Grad unter allen normierten Polynomen mit Nullstelle e. Man hat dann einen injektiven Homomorphismus der kommutativen R-Algebra $C := R[X]/(f)$ in Z vermöge $X \mapsto e$, und $\underline{c} := C \cap \underline{z}$ ist ein Ideal in $C \subseteq Z$. $e+\underline{c}$ ist ein Idempotent in $C/\underline{c}$ und kann nach Voraussetzung zu einem Idempotent d von C gehoben werden. Wegen des induzierten injektiven Homomorphismus $C/\underline{c} \longrightarrow Z/\underline{z}$ ist d ein Idempotent, welches $d - e \in \underline{z}$ erfüllt. (C)$\Rightarrow$(A) gilt a fortiori.

§ 4 ANWENDUNG DER UNIVERSELLEN ZERFÄLLUNGS-ALGEBRA FÜR SEPARABLE POLYNOME

Definition 4.1

Das normierte Polynom f über dem Ring R heißt separabel, wenn $R[X]/(f)$ eine separable R-Algebra ist.

(Nach M.Auslander und O.Goldman [1] heißt eine kommutative R-Algebra B separabel, falls sie ein projektiver $B \otimes_R B$-Modul ist.)

Falls R ein Körper ist, fällt die obige Definition mit der üblichen zusammen, nach der ein Polynom separabel ist, wenn es keine mehrfachen Nullstellen in einem algebraischen Abschluß von R besitzt (vgl [3, Th.2.2.5 und Th.2.7.1]).

Für jedes normierte Polynom $f \in R[X]$ kann man wie in der Körpertheorie die Diskriminante definieren (vgl. [18, § 33]).

Lemma 4.2

Für jedes normierte Polynom $f \in R[X]$ ist

$$D(f) := \prod_{i<j} (z_i - z_j)^2$$

(wo i,j von 1 bis n=grad(f) laufen und $z_i \in Z(f,R)$ mit den Bezeichnungen von 1.1 ist) ein Element in R.

Beweis: Da $\prod_{i<j} (X_i - X_j)^2$ ein Element von $R[s_1,\ldots,s_n]$

ist, gilt $D(f) \in R[s_1,\ldots,s_n]/\underline{a} \cap R[s_1,\ldots,s_n] \cong R \cdot 1_{Z(f,R)} \cong R$.

In [4] wendet T.Nagahara die universelle Zerfällungsalgebra auf ein Resultat von Janusz [9] an und erhält:

Satz 4.3
Das normierte Polynom $f \in R[X]$ ist genau dann separabel, wenn $D(f)$ in R invertierbar ist.
Beweis: vgl. [14, Th. 2.2].

Das folgende Lemma dient zum Beweis von Satz 4.7.

Lemma 4.4
Das normierte Polynom $f \in R[X]$ sei separabel. Wenn $f = g \cdot h$ mit zwei normierten Polynomen über einer R-Algebra B gilt, so sind g und h separabel über B.
Beweis: Der Beweis könnte mit 4.3 geführt werden; wir wollen anders schließen. Aus der Separabilität von $R[X]/(f)$ folgt nach [3, Cor. 2.1.7] wegen der Kommutativität von B die Separabilität der B-Algebra $B \otimes_R R[X]/(f) \cong B[X]/(f)$. Nach [3, Prop. 2.1.11] sind dann auch $B[X]/(g)$ und $B[X]/(h)$ als epimorphe Bilder von $B[X]/(f)$ separabel über B. Nach 4.1 folgt daraus die Behauptung.

Bemerkung 4.5 Die Umkehrung gilt i.a. nicht, denn f^2

ist nicht separabel, falls f separabel ist und positiven Grad hat.

Beweis: Mit 4.3 und dem Epimorphismus $Z(f^2,R) \longrightarrow Z(f,R)$, welcher nach 1.2 existiert.

Folgerung 4.6

Mit den Bezeichnungen von 1.3 gilt: Falls f ein separables Polynom in $R[X]$ ist, sind die Polynome f_i separabel über R_i. Nach 4.1 gilt dann für alle $i=1,\ldots,n$: R_i ist eine separable R_{i-1}-Algebra. Nach [3, Prop.2.1.12] ist dann aus Transitivitätsgründen auch $Z(f,R) \cong R_n$ eine separable R-Algebra.

Jetzt können wir den Satz beweisen:

Satz 4.7

Das normierte Polynom $f \in R[X]$ ist genau dann separabel, wenn die universelle Zerfällungsalgebra $Z(f,R)$ eine separable R-Algebra ist.

Beweis: Wegen Folgerung 4.6 haben wir nur noch zu zeigen, daß mit $Z(f,R)$ auch f separabel ist. Sei also $Z(f,R)$ separabel über R. Mit den Bezeichnungen von 1.3 gilt $R_{n-1} \cong R_n \cong Z(f,R)$, denn $R_n = R_{n-1}[X]/(f_{n-1})$ und f_{n-1} hat den Grad 1. Nach [3, Prop. 2.1.12] ist $Z(f,R)$ separabel über R_{n-2}. Folglich ist R_{n-1} separabel über R_{n-2} und daher f_{n-2} separabel über R_{n-2} nach 4.1.

Nach 1.3 und 1.4 ist $f_{n-2} = (X - z_{n-1})(X - z_n)$ (weil normierte Polynome keine Nullteiler sind), so daß nach 4.3 $D(f_{n-2}) = (z_{n-1} - z_n)^2$ in R_{n-2} invertierbar ist. Mit der n-fachen Transitivität der S_n folgt mit 1.7 aus der Invertierbarkeit von $(z_{n-1} - z_n)$ die Invertierbarkeit von $(z_i - z_j)$ in $Z(f,R)$ für alle $i \neq j$. Also ist $D(f)$ in $Z(f,R)$ invertierbar.

Nun ist wegen der S_n-Normalität von $Z(f,R)$ (vgl. 2.5) aber $\prod_{\sigma \in S_n} \sigma(1/D(f))$ in R. Also ist wegen

$$(D(f))^{n!-1} \cdot \prod_{\sigma \in S_n} \sigma(1/D(f)) = \prod_{\substack{\sigma \in S_n \\ \sigma \neq 1}} \sigma(D(f)) \cdot \prod_{\sigma \in S_n} \sigma(1/D(f))$$

$= 1/D(f)$ auch $1/D(f)$ in R, d.h. f ist separabel über R.

§ 5 DIE AUTOMORPHISMENGRUPPE VON Z(f,R) ÜBER EINEM ZUSAMMENHÄNGENDEN RING R

Wir schicken einige Lemmata voraus.

Lemma 5.1

Sei $\varphi: Z(f,R) \longrightarrow B$ ein Epimorphismus auf die R-Algebra B und $F_\varphi := \{\sigma \in \mathrm{Aut}_R Z(f,R) : \sigma(\ker\varphi) = \ker\varphi\}$. Man hat einen natürlichen Homomorphismus φ^* von F_φ in $\mathrm{Aut}_R B$.

Beweis: Wenn $\sigma \in F_\varphi$, so ist $\ker\varphi\sigma = \ker\varphi$, also existiert $\tau \in \mathrm{End}_R B$ mit $\tau\varphi = \varphi\sigma$. τ ist surjektiv, weil $\varphi\sigma$ surjektiv ist; τ ist injektiv, weil $\ker\tau\varphi = \ker\varphi\sigma = \sigma^{-1}(\ker\varphi) = \ker\varphi$ und weil φ surjektiv ist. Also ist $\tau \in \mathrm{Aut}_R B$, und τ ist durch $\tau\varphi = \varphi\sigma$ eindeutig bestimmt. Die Zuordnung $\sigma \longmapsto \tau$ ist ein Homomorphismus, weil aus $\tau\varphi = \varphi\sigma$ und $\tau'\varphi = \varphi\sigma'$ folgt, daß $\tau\tau'\varphi = \tau\varphi\sigma' = \varphi\sigma\sigma'$ gilt.

Lemma 5.2

Wenn mit den Bezeichnungen von 5.1 die Zerlegung $f(X) = \prod_{j=1}^{n}(X - \varphi(z_j))$ des Polynoms $f \in R[X]$ in Linearfaktoren über B eindeutig ist, so ist die Einschränkung von φ^* auf $F_\varphi \cap \mathfrak{S}_n$ (vgl. Bezeichnung 1.7) ein Epimorphismus.

Beweis: Sei $\tau \in \mathrm{Aut}_R B$; nach Voraussetzung existiert $\pi \in S_n$ mit $\tau(\varphi(z_j)) = \varphi(z_{\pi(j)})$ für alle $j=1,\ldots,n$. Mit $\bar{\pi} \in \mathfrak{S}_n \subseteq \mathrm{Aut}_R Z(f,R)$ gilt also für alle $j=1,\ldots,n$ $\tau\varphi(z_j) = \varphi\bar{\pi}(z_j)$, also wegen $Z(f,R) = R[z_1,\ldots,z_n]$

$\tau\varphi = \varphi\bar{\pi}$. Wir zeigen $\bar{\pi} \in F$; wegen $\varphi\bar{\pi}(\ker\varphi) = \tau\varphi(\ker\varphi) = 0$ folgt $\bar{\pi}(\ker\varphi) \subseteq \ker\varphi$ und wegen $\varphi\bar{\pi}^{-1}(\ker\varphi) = \tau^{-1}\varphi(\ker\varphi) = 0$ folgt $\ker\varphi \subseteq \bar{\pi}(\ker\varphi)$.

Lemma 5.3

Der Kern des Homomorphismus $\varphi^*: F_\varphi \longrightarrow \mathrm{Aut}_R B$ ist $\{\sigma \in \mathrm{Aut}_R Z(f,R) : \forall\, j=1,\ldots,n \;\; (\sigma(z_j) - z_j) \in \ker\varphi\}$.

Beweis: Aus $\sigma \in \ker\varphi^*$ folgt $\varphi\sigma = \varphi$, also für alle $j = 1,\ldots,n$ $\sigma(z_j) - z_j \in \ker\varphi$. Ist umgekehrt $\sigma \in \mathrm{Aut}_R Z(f,R)$ so, daß für alle $j=1,\ldots,n$ $\sigma(z_j) - z_j \in \ker\varphi$ ist, so folgt wegen $Z(f,R) = R[z_1,\ldots,z_n]$ $\varphi\sigma = \varphi$. Wir zeigen $\sigma \in F_\varphi$; aus $\varphi\sigma(\ker\varphi) = \varphi(\ker\varphi) = 0$ folgt $\sigma(\ker\varphi) \subseteq \ker\varphi$. Wegen $\sigma(z_j) - z_j \in \ker\varphi \iff \sigma^{-1}(z_j) - z_j \in \ker\varphi$ folgt $\varphi\sigma^{-1} = \varphi$ und deshalb $\varphi\sigma^{-1}(\ker\varphi) = \varphi(\ker\varphi) = 0$, d.h. $\ker\varphi \subseteq \sigma(\ker\varphi)$.

Lemma 5.4

Wenn mit den Bezeichnungen der vorangehenden Lemmata $\{b_1,\ldots,b_m\} := \{\varphi(z_j) : j=1,\ldots,n\}$ eine m-elementige Menge und c_i $(i=1,\ldots,m)$ die Anzahl derjenigen z_j ist, für welche $\varphi(z_j) = b_i$ gilt, so ist, falls $\bar{S}_n \cong S_n$ gilt:

$$\left|\ker\varphi^* \cap \bar{S}_n\right| = \prod_{i=1}^{m} c_i!$$

Beweis: Nach Voraussetzung ist $\bar{S}_n$ isomorph zu S_n. Nach 5.3 besteht dann $\ker\varphi^* \cap \bar{S}_n$ genau aus denjenigen Permutationen von $\bar{S}_n$, welche die Kongruenz modulo $\ker\varphi$ respektieren, d.h. welche die Mengen $\{z_j : j=1,\ldots,n\} \cap \varphi^{-1}(b_i)$

komplexweise festlassen. Diese Mengen haben jeweils die Mächtigkeit c_i und daraus folgt die Behauptung.

Definition 5.5

Ein Ring, welcher nur die trivialen Idempotenten 0 und 1 besitzt, heißt zusammenhängend.

Lemma 5.6 (Dress[4])

Sei B eine G-normale (R,G)-Algebra und $R\cdot 1_B$ zusammenhängend. 1_B besitzt eine feinste Zerlegung $T=\{e_1,\dots,e_k\}$ in orthogonale primitive Idempotente, $1_B = e_1 + \cdots + e_k$, und G wirkt transitiv auf dieser Zerlegung.

Beweis: Wir folgen dem Beweis von A.Dress in [4].

Jede orthogonale Zerlegung von 1_B besitzt eine G-invariante Verfeinerung; es genügt nämlich, das Produkt $1_B = \prod_{\gamma\in G} \gamma(e_1 + \cdots + e_m)$ auf der rechten Seite auszumultiplizieren. Wenn $1_B = e_1 + \cdots + e_m$ eine Zerlegung in orthogonale Idempotente war, so ist die angegebene Verfeinerung G-invariant und ebenfalls orthogonal.

G wirkt auf jeder G-invarianten orthogonalen Zerlegung $1_B = e_1 + \cdots + e_m$ transitiv. Wegen der G-Normalität ist nämlich das Element $r := \sum_{\gamma\in G/D} \gamma\left(\prod_{\delta\in D} \delta(e_1)\right) = \sum_{\gamma\in G/D} \gamma(e_1)$ in $R\cdot 1_B$, wenn $D = \{\delta\in G: \delta(e_1) = e_1\}$ und G/D ein Vertretersystem von Linksnebenklassen von D in G ist. r ist ein Idempotent in $R\cdot 1_B$ und deshalb $= 1_B$. Daraus folgt,

daß die Summe aller Konjugierten von e_1 gleich $e_1 + \cdots + e_m$ ist.

Da je zwei orthogonale 1_B-Zerlegungen eine gemeinsame G-invariante Verfeinerung besitzen, kann wegen der Transitivität von G jede orthogonale 1_B-Zerlegung höchstens $|G|$ Elemente besitzen. Also gibt es eine feinste (und nur eine feinste) Zerlegung von 1_B in orthogonale Idempotente, welche offenbar primitiv sind. Wie oben gezeigt, wirkt G transitiv auf dieser Zerlegung.

Satz 5.7

Sei B eine R-Algebra und $1_B = e_1 + \cdots + e_k$ eine Zerlegung des Einselements in orthogonale Idempotente, auf denen $\mathrm{Aut}_R B$ transitiv durch Permutieren wirkt. Die Automorphismengruppe $\mathrm{Aut}_R B$ ist eine zerfallende Erweiterung von $\prod_{i=1}^{k} \mathrm{Aut}_R Be_i$ durch die symmetrische Gruppe S_k und die Gruppen $\mathrm{Aut}_R Be_i$ sind isomorph.

Beweis: Da jedes $\varrho \in \mathrm{Aut}_R B$ die Idempotenten permutiert, gibt es einen Homomorphismus $\alpha: \mathrm{Aut}_R B \longrightarrow S_k$, wenn man $\alpha(\varrho) := \pi$ setzt, falls $\varrho(e_i) = e_{\pi(i)}$ für alle $i = 1,\ldots,k$ gilt. Aus der Orthogonalität der Idempotenten folgt $B = \prod_{i=1}^{k} Be_i$ (direktes Produkt der Ideale Be_i). Der Kern von α besteht aus genau denjenigen Automorphismen, welche Be_i auf Be_i $(i=1,\ldots,k)$ abbilden. Man hat daher einen Monomorphismus γ von $\ker\alpha$ in $\prod_{i=1}^{k} \mathrm{Aut}_R Be_i$, welcher durch $\gamma(\varrho) := (\varrho|_{Be_1},\ldots,\varrho|_{Be_k})$

definiert ist. γ ist ein Isomorphismus, weil man bei Vorgabe von Automorphismen der einzelnen Komponenten Be_i stets durch Zusammensetzen einen Automorphismus von ganz B erhält.

Wir werden nun einen Homomorphismus β von S_k in $Aut_R B$ definieren mit den Eigenschaften

(i) $\alpha \cdot \beta = id_{S_k}$

(ii) $\ker \alpha \cap \beta(S_k) = 1$

(iii) $\ker \alpha \cdot \beta(S_k) = Aut_R B$

Aus (i) folgt dann, daß β ein Monomorphismus ist. Identifiziert man also $\ker \alpha$ mit $\prod_{i=1}^{k} Aut_R Be_i$ vermöge γ und S_k mit seinem Bild $\beta(S_k)$, so ist $\prod_{i=1}^{k} Aut_R Be_i$ Normalteiler in $Aut_R B$ und deshalb $Aut_R B$ zerfallende Erweiterung von $\prod_{i=1}^{k} Aut_R Be_i$ durch S_k.

β erhalten wir auf die folgende Weise:

Da $Aut_R B$ transitiv auf den Idempotenten e_i wirkt, gibt es $\varrho_i \in Aut_R B$ mit $\varrho_i(Be_1) = Be_i$. Wir setzen für $\pi \in S_k$ $\beta(\pi) := \varrho$, wo ϱ durch

$$\varrho|_{Be_i} := \varrho_{\pi(i)}|_{Be_1} \cdot \varrho_i^{-1}|_{Be_i}$$

auf den einzelnen Komponenten Be_i definiert wird. Wie man leicht nachprüft ist $\varrho \in Aut_R B$. Die Abbildung β ist ein Homomorphismus, denn wenn π auf ϱ und π' auf ϱ' abgebildet wird, so wird $\pi\pi'$ auf $\varrho\varrho'$ abgebildet, weil

$$\varrho\varrho'|_{Be_i} = \varrho|_{Be_{\pi(i)}} \cdot \varrho'|_{Be_i} =$$

$$\varrho_{\pi\pi'(i)}|_{Be_1} \cdot \varrho_{\pi'(i)}^{-1}|_{Be_{\pi'(i)}} \cdot \varrho_{\pi'(i)}|_{Be_1} \cdot \varrho_i^{-1}|_{Be_i} =$$

$= \rho_{\pi\pi'(i)}\big|_{Be_1} \cdot \rho_i^{-1}\big|_{Be_i}$.

Daß β die Eigenschaften (i) und (ii) erfüllt, ist klar. Wir zeigen jetzt Eigenschaft (iii). Sei $\varphi \in Aut_R B$; dann ist $\varphi = \gamma^{-1}(\tau_1,\ldots,\tau_k) \cdot \beta\alpha(\varphi)$, wo $\tau_i = \varphi\big|_{Be_{\alpha(\varphi^{-1}(i))}} \cdot \beta\alpha(\varphi^{-1})\big|_{Be_i}$.

Es ist nämlich $\tau_i \in Aut_R Be_i$, weil $\varphi \cdot \beta\alpha(\varphi^{-1})(e_i) = \varphi\varphi^{-1}(e_i)$ $= e_i$, und es ist $\left(\gamma^{-1}(\tau_1,\ldots,\tau_k) \cdot \beta\alpha(\varphi)\right)\big|_{Be_i} =$ $\gamma^{-1}(\tau_1,\ldots,\tau_k)\big|_{Be_{\alpha(\varphi)(i)}} \beta\alpha(\varphi)\big|_{Be_i} = \tau_{\alpha(\varphi)(i)} \cdot \beta\alpha(\varphi)\big|_{Be_i} =$ $\varphi\big|_{Be_i} \cdot \beta\alpha(\varphi^{-1})\big|_{Be_{\alpha(\varphi)(i)}} \cdot \beta\alpha(\varphi)\big|_{Be_i} = \varphi\big|_{Be_i}$.

Die Abbildung $\tau \longrightarrow (\rho_i \cdot \tau \cdot \rho_i^{-1})\big|_{Be_i}$ liefert offenbar einen Isomorphismus von $Aut_R Be_1$ auf $Aut_R Be_i$. Damit ist alles bewiesen.

Folgerung 5.8

Sei B eine G-normale (R,G)-Algebra, $R \cdot 1_B$ zusammenhängend. Wenn $1_B = e_1 + \cdots + e_k$ die feinste orthogonale Zerlegung des Einselements ist (nach Lemma 5.6), so ist $Aut_R B$ eine zerfallende Erweiterung von $\prod_{i=1}^{k} Aut_R Be_i$ durch S_k.

$T = \{e_1,\ldots,e_k\}$ ist die Menge der Blockidempotenten von B.

Beweis: Lemma 5.6 und Satz 5.7.

Folgerung 5.9

Sei f ein normiertes Polynom vom Grad n über dem zusammenhängenden Ring R und $T = \{e_1,\dots,e_k\}$ die Menge der Blockidempotenten von $Z = Z(f,R)$. $\mathrm{Aut}_R Z$ ist zerfallende Erweiterung einer Untergruppe $U \cong \prod_{i=1}^{k} \mathrm{Aut}_R Ze_i$ durch die symmetrische Gruppe S_k.

Für die Anzahl k der Blockidempotenten gilt $k \geqslant n$ oder genau eine der folgenden Aussagen

(a) $k = 1$ und $U \cap \overline{S}_n = \overline{S}_n$, $U = \mathrm{Aut}_R Z$

(b) $k = 2$ und $U \cap \overline{S}_n = \overline{A}_n$,

(c) $k = 3$, $n = 4$ und $U \cap \overline{S}_4 = \overline{V}_4$.

Dabei bedeuten S_n, A_n, V_4 die symmetrische Gruppe bzw. die alternierende Gruppe bzw. die Kleinsche Vierergruppe und $\overline{S}_n$, $\overline{A}_n$, $\overline{V}_4$ ihre (nach 1.8) für $n \neq 2$ isomorphen Bilder in $\mathrm{Aut}_R Z$.

Beweis: Die erste Hälfte der Behauptung folgt aus 5.8. Da U Normalteiler von $\mathrm{Aut}_R Z$ ist, ist $U \cap \overline{S}_n$ Normalteiler von $\overline{S}_n$. Falls $U \cap \overline{S}_n = 1$ ist, folgt $\overline{S}_n \cong \overline{S}_n / U \cap \overline{S}_n = U \cdot \overline{S}_n / U \leqslant \mathrm{Aut}_R Z / U \cong S_k$ daraus folgt für $\overline{S}_n \cong S_n$ $n! \leqslant k!$, also $n \leqslant k$. Falls $\overline{S}_n \neq S_n$, ist $n=2$; wenn nicht $n \leqslant k$ ist, tritt Fall (a) ein, denn dann ist $k=1$, also $U = \mathrm{Aut}_R Z$ und daher $U \cap \overline{S}_n = \overline{S}_n$.

Sei also $U \cap \overline{S}_n \neq 1$; setzt man für alle $i = 1,\dots,k$ $\overline{F}_i := \{\sigma \in \overline{S}_n : \sigma(e_i) = e_i\}$, so gilt wegen der Beziehung $U = \{\sigma \in \mathrm{Aut}_R Z : \forall\, i=1,\dots,k \;\; \sigma(e_i) = e_i\}$ (vgl. 5.7) $U \cap \overline{S}_n = \bigcap_{i=1}^{k} \overline{F}_i$ und $k = (\overline{S}_n : \overline{F}_1)$, weil S_n nach 5.6 transitiv auf den Idempotenten wirkt.

$\overline{F}_1$ ist eine Untergruppe von $\overline{S}_n$, welche den Normalteiler $U \cap \overline{S}_n$ enthält.

Für $n \neq 4$ hat S_n nur die Normalteiler S_n, A_n und 1; Wegen $\overline{S}_n \cong S_n$ für $n \neq 2$ folgt daraus, daß für $n \neq 4$ auch $\overline{S}_n$ nur die Normalteiler $\overline{S}_n, \overline{A}_n$ und 1 besitzt. Für $n \neq 4$ bleiben daher nur die Möglichkeiten $U \cap \overline{S}_n = \overline{S}_n$ und $U \cap \overline{S}_n = \overline{A}_n$; also bleiben für $\overline{F}_1$ nur die Möglichkeiten $\overline{F}_1 = \overline{S}_n$ (dann gilt (a)) oder $\overline{F}_1 = \overline{A}_n$ (dann gilt (b)). Die Behauptung ist damit für $n \neq 4$ bewiesen.

Für $n=4$ gibt es außer den Möglichkeiten $\overline{F}_1 = \overline{S}_4$, $\overline{F}_1 = \overline{A}_4$ (d.h. Fall (a) bzw. Fall (b)) für $k < n$ noch die Möglichkeit, daß $k=3$ und $\overline{F}_1$ eine der 2-Sylow-Gruppen von $\overline{S}_4$ ist. Da die Gruppen $\overline{F}_i$ konjugiert sind, folgt dann $U \cap \overline{S}_4 = \bigcap_{i=1}^{3} \overline{F}_i = \overline{V}_4$, d.h. es gilt (c).

Bemerkung 5.10

Wenn der Ring R lokal (also zusammenhängend) ist, so ist jedes der Ideale Ze_i ein freier R-Modul der Dimension $n!/k$. Dann folgt aus $k \geq n$, daß $k \leq (n-1)!$ ist.

Beweis: Die Ideale Ze_i sind isomorph als R-Algebren und projektiv als direkte Summanden eines freien R-Moduls. Weil R lokal ist, sind es freie R-Moduln (vgl. [10, III, 8., Lemma 3]).

Folgerung 5.11

Wenn unter den Voraussetzungen und mit den Bezeichnungen von 5.9 R ein Körper ist, so gilt für $Z = Z(f,R)$ $\mathrm{Aut}_R Z / \ker \varphi^* \cong \mathrm{Aut}_R(Z/\mathrm{Rad}(Z))$ und $\mathrm{Aut}_R(Z/\mathrm{Rad}(Z))$ ist zerfallende Erweiterung einer Untergruppe $U^* \cong \prod_{i=1}^{k} \mathrm{Gal}(K:R)$ durch die symmetrische Gruppe S_k, wobei K der Zerfällungskörper von f und φ^* der zum Homomorphismus $\varphi: Z \longrightarrow Z/\mathrm{Rad}(Z)$ gehörende Homomorphismus ist (vgl. 5.1).

Beweis: Sei $\overline{Z} = Z/\mathrm{Rad}(Z)$ und $\overline{e}_i := \varphi(e_i)$ für alle $i = 1,\ldots,k$. Da Rad(Z) keines der Blockidempotenten e_i von Z enthält, hat $\overline{Z}$ ebenfalls k Blockidempotente $\overline{e}_i$.

Zum Beweis der zweiten Hälfte der Behauptung genügt es zu zeigen, daß $\overline{Z}\overline{e}_i$ für alle $i=1,\ldots,k$ isomorph zu K ist. Denn da Rad(Z) unter allen Automorphismen invariant ist, erfüllt $\overline{Z}$ nach 2.4 die Voraussetzungen von 5.8 mit der Gruppe S_n. Als epimorphes Bild des Artin-Ringes Z (Z ist endlich-dimensionaler Vektorraum über R) ist $\overline{Z}\overline{e}_i$ ein Artin-Ring und daher lokal. Wegen $\mathrm{Rad}(\overline{Z}\overline{e}_i)=0$ ist $\overline{Z}\overline{e}_i$ ein Körper, welcher von den Wurzeln von f erzeugt wird; folglich ist $\overline{Z}\overline{e}_i \cong K$.

Da Rad(Z) invariant unter allen Automorphismen von Z ist, gilt mit den Bezeichnungen von 5.1 $F_\varphi = \mathrm{Aut}_R Z$.

Zum Beweis der ersten Hälfte der Behauptung zeigen wir, daß φ^* ein Epimorphismus auf $\mathrm{Aut}_R \overline{Z}$ ist.

Nach 5.9 ist $\mathrm{Aut}_R Z = U \cdot \overline{S}_k$, wo $\overline{S}_k$ eine Untergruppe von $\mathrm{Aut}_R Z$ ist, welche zu S_k isomorph ist unter $\alpha: \overline{S}_k \longrightarrow S_k$

mit $\bar{\sigma}(e_i) = e_{\alpha(\bar{\sigma})(i)}$ für die Blockidempotenten e_i. Das Bild S'_k von $\bar{S}_k$ unter φ^* ist ebenfalls isomorph zu S_k, weil $\varphi^*(\bar{\sigma})(\bar{e}_i) = \varphi(\bar{\sigma}(e_i)) = \bar{e}_{\alpha(\bar{\sigma})(i)}$ und $\bar{Z}$ ebenfalls k Blockidempotente besitzt.

Wegen $U = \{\sigma \in \mathrm{Aut}_R Z : \forall i=1,\dots,k \ \sigma(e_i) = e_i\}$ und $U^* = \{\sigma \in \mathrm{Aut}_R \bar{Z} : \forall\ i=1,\dots,k \ \sigma(\bar{e}_i) = \bar{e}_i\}$ gilt sicherlich $\varphi^*(U) \subseteq U^*$. Wenn wir $\varphi^*(U) = U^*$ zeigen können, sind wir fertig, denn dann ist $\varphi^*(\mathrm{Aut}_R Z) = \varphi^*(U \cdot \bar{S}_k) = U^* \cdot S'_k$ und es ist wegen $U^* \cap S'_k = 1$ $U^* \cdot S'_k = \mathrm{Aut}_R \bar{Z}$, also φ^* surjektiv.

Sei also $\tau \in U^*$ und wie im Beweis zu Satz 5.7 γ der Isomorphismus von U auf $\prod_{i=1}^{k} \mathrm{Aut}_R Ze_i$. Sei $\tau_i = \tau|_{\bar{Ze}_i}$; dann ist $(\tau_1,\dots,\tau_k)$ das Bild von τ bei dem Isomorphismus von U^* auf die Gruppe $\prod_{i=1}^{k} \mathrm{Aut}_R \bar{Z}\bar{e}_i \cong \prod_{i=1}^{k} \mathrm{Gal}(K:R)$. Sei ψ_i der Epimorphismus von $\bar{Z}$ auf $\bar{Z}\bar{e}_i \cong K$; dann ist $\psi_i(\bar{e}_j)=0$ für $j \neq i$ und $\psi_i|_{\bar{Ze}_i} = \mathrm{id}_{\bar{Ze}_i}$.

Wendet man Lemma 5.2 auf den Epimorphismus $\psi_i\varphi$ an, so erhält man für alle $i=1,\dots,k$ zu dem Automorphismus $\tau_i \in \mathrm{Aut}_R \bar{Z}\bar{e}_i \cong \mathrm{Gal}(K:R)$ ein $\rho_i \in \mathrm{Aut}_R Z$ mit $\rho_i(\ker\psi_i\varphi) = \ker\psi_i\varphi$ und $\psi_i\varphi\rho_i = \tau_i\psi_i\varphi$. Offenbar ist $\rho_i(\ker\psi_i\varphi) = \ker\psi_i\varphi$ gleichbedeutend mit $\rho_i(e_i) = e_i$.

Sei nun $\rho := \gamma^{-1}(\rho_1|_{Ze_1},\dots,\rho_k|_{Ze_k})$; wegen $(\varphi\rho)|_{Ze_i} = \varphi|_{Ze_i} \cdot \rho_i|_{Ze_i} = \psi_i|_{\bar{Ze}_i} \cdot \varphi|_{Ze_i} \cdot \rho_i|_{Ze_i} = (\psi_i\varphi\rho_i)|_{Ze_i} = (\tau_i\psi_i\varphi)|_{Ze_i} = \tau_i \cdot \psi_i|_{\bar{Ze}_i} \cdot \varphi|_{Ze_i} = \tau_i \cdot \varphi|_{Ze_i} = (\tau\varphi)|_{Ze_i}$ ist $\varphi^*(\rho) = \tau$, wie zu zeigen war.

§ 6 DIE DIMENSION DES RADIKALS VON Z(f,R) ÜBER EINEM KÖRPER R

In diesem Abschnitt sei R stets ein Körper und K der Zerfällungskörper des normierten Polynoms f vom Grad n über R.

Lemma 6.1

Sei φ ein R-Epimorphismus von Z(f,R) auf K und $f(X) = \prod_{i=1}^{l} g_i^{e_i}(X)$ eine Primfaktorzerlegung von f mit normierten Polynomen $g_i(X) \in R[X]$.

Mit den Bezeichnungen von Lemma 5.1 gilt, falls $\overline{S}_n \cong S_n$ ist: $|\ker\varphi^* \cap \overline{S}_n| = \prod_{i=1}^{l} ((e_i \cdot p^{m_i})!)^{\text{grad } g_i / p^{m_i}}$

wobei p^{m_i} der Inseparabilitätsgrad von $g_i(X)$ über R ist.

Beweis: Jedes irreduzible Polynom $g(X) \in R[X]$ läßt sich schreiben $g(X) = \overline{g}(X^{p^m})$, wo $\overline{g}(Y)$ ein separables Polynom in R[Y] und m=0 für charR = 0 bzw. $m \in \mathbb{N} \cup \{0\}$ für charR = p ist. p^m ist der Inseparabilitätsgrad von g(X) über R. Mit dieser Bezeichnungsweise ist also für alle i=1,...,l $g_i(X) = \overline{g}_i(X^{p^{m_i}})$ und grad $\overline{g}_i$ = grad g_i/p^{m_i}. Nach Lemma 5.4 genügt zur Bestimmung von $|\ker\varphi^* \cap \overline{S}_n|$ die Kenntnis der Vielfachheiten c_j der Wurzeln von f in K. Aus der Primfaktorzerlegung von f folgt, daß für $i \neq j$ die Polynome $g_i(X)$ und $g_j(X)$ keine gemeinsame Wurzel in K besitzen. Daher kann man die Vielfachheiten

der Wurzeln für jedes Primpolynom $g_i(X)$ getrennt berechnen.
Mit der obigen Bemerkung über die Inseparabilitätsgrade gilt: $g_i(X)$ hat grad $\bar{g}_i(Y)$ verschiedene Wurzeln in K mit der jeweiligen Vielfachheit p^{m_i}. Also hat $g_i^{e_i}(X)$ ebensoviel verschiedene Wurzeln mit der jeweiligen Vielfachheit $e_i \cdot p^{m_i}$. Mit Lemma 5.4 erhält man daraus für $\overline{S}_n \cong S_n$ die angegebene Ordnung.

Da R ein Körper ist, erfüllt $Z = Z(f,R)$ die Voraussetzungen von 5.9; sei k die Anzahl der Blockidempotenten von Z und p^s der Inseparabilitätsgrad von K über R. Mit den Bezeichnungen von Lemma 6.1 gilt:

Lemma 6.2

(a) $\dim_R \mathrm{Rad}(Z) = \dim_R Z - k \cdot \dim_R K$

(b) $\dim_R \mathrm{Rad}(Z) = n! - n! \cdot p^s / \prod_{i=1}^{l} ((e_i \cdot p^{m_i})!)^{\mathrm{grad}\, g_i / p^{m_i}}$

Beweis: Sei $T = \{\tilde{e}_1, \ldots, \tilde{e}_k\}$ die Menge der Blockidempotenten von Z. Für alle i ist $Z\tilde{e}_i$ ein zusammenhängender Ring. Als epimorphes Bild des Artin-Ringes Z ist $Z\tilde{e}_i$ ein Artin-Ring, also lokal. Der Restklassenkörper von $Z\tilde{e}_i$ ist als epimorphes Bild von Z isomorph zum Zerfällungskörper K von f. Folglich ist $\dim_R \mathrm{Rad}(Z) = \sum_{i=1}^{k} (\dim_R Z\tilde{e}_i - \dim_R K) = \dim_R Z - k \cdot \dim_R K$.
Zum Beweis von (b) sei φ wie in 6.1 ein R-Epimorphis-

mus von Z auf K (vgl. Satz 1.2). Es gibt genau ein Idempotent aus T, welches auf $1 \in K$ abgebildet wird. Sei o.B.d.A. $\varphi(\tilde{e}_1) = 1$; dann ist mit den Bezeichnungen aus Lemma 5.1 und aus dem Beweis von 5.9 $\overline{F}_1 = F_\varphi \cap \overline{S}_n$. Aus $k = (\overline{S}_n : \overline{F}_1)$ folgt mit $\dim_R Z = n!$ (nach 1.5) aus (a) $\dim_R \mathrm{Rad}(Z) = n! - |\overline{S}_n| \cdot \dim_R K \,/\, |(F_\varphi \cap \overline{S}_n)|$. Nun ist bekanntlich $\dim_R K = p^s \cdot |\mathrm{Gal}(K:R)|$, wo $\mathrm{Gal}(K:R)$ die Galois-Gruppe von K über R ist. Da K nullteilerfrei ist, ist nach Lemma 5.2 die Einschränkung von φ^* auf $F_\varphi \cap \overline{S}_n$ ein Epimorphismus auf $\mathrm{Gal}(K:R)$. Folglich ist $(F_\varphi \cap \overline{S}_n) \,/\, \ker \varphi^* \cap \overline{S}_n \cong \mathrm{Gal}(K:R)$. Mit der obigen Formel folgt daher $\dim_R \mathrm{Rad}(Z) = n! - |\overline{S}_n| \cdot p^s \,/\, |\ker \varphi^* \cap \overline{S}_n|$. Wenn $\overline{S}_n \cong S_n$ ist, folgt mit Lemma 6.1 die Formel (b). Wenn $\overline{S}_n \ncong S_n$, so ist nach Bemerkung 1.9 n=2, charR = 2 und f von der Form $X^2 + a$. Je nachdem, ob f über R irreduzibel ist oder nicht, unterscheidet man die beiden Möglichkeiten (i) k=1, $\dim_R K = 2$, $p^s=2$, l=1, $e_1=1$, $p^{m_1}=2$ und (ii) k=2, K=R, $p^s=1$, l=1, $e_1=2$, $p^{m_1}=1$. In beiden Fällen folgert man aus (a) sofort die Richtigkeit von Formel (b).

Satz 6.3

Z(f,R) ist halbeinfach genau dann, wenn gilt:

(i) f(X) ist ein Produkt von paarweise verschiedenen irreduziblen normierten Polynomen $g_i(X) \in R[X]$, welche entweder separabel oder quadratisch - inseparabel sind, und

(ii) der Inseparabilitätsgrad von K über R ist 2^r, wo r die Anzahl der quadratisch-inseparabeln Polynome $g_i(X)$ ist.

Wenn char $R \neq 2$ ist, so ist $Z(f,R)$ halbeinfach genau dann, wenn $f(X)$ Produkt von paarweise verschiedenen irreduziblen separablen Polynomen $g_i(X) \in R[X]$ ist.

Beweis: Sei $u := \prod_{i=1}^{l}((e_i \cdot p^{m_i})!)^{\text{grad } g_i/p^{m_i}}$. Nach Lemma 6.2 gilt für $Z = Z(f,R)$ $\dim_R \text{Rad}(Z) = 0 \iff p^s = u$. Aus der Tatsache, daß sich die Inseparabilitätsgrade bei Körpererweiterungen multiplizieren, folgt sofort $p^s \leq \prod_{i=1}^{l} p^{m_i}$. Da offensichtlich $\prod_{i=1}^{l} p^{m_i} \leq u$ ist, gilt

$$\text{Rad}(Z) = 0 \iff \left(p^s = \prod_{i=1}^{l} p^{m_i} \text{ und } u = \prod_{i=1}^{l} p^{m_i} \right).$$

Die rechte Seite sei erfüllt; wir zeigen (i) und (ii). Aus $u = \prod_{i=1}^{l} p^{m_i}$ folgt, daß $e_i = 1$ für alle $i=1,\ldots,l$ ist, weil andernfalls $(e_i \cdot p^{m_i})! > p^{m_i}! \geq p^m$ ist. Weiter muß $1 \leq p^{m_i} \leq 2$ für alle $i=1,\ldots,l$ sein, weil andernfalls $p^{m_i}! > p^{m_i}$ ist. Wenn $p^{m_i} = 2$ ist, so muß grad $g_i = 2$ sein, weil andernfalls $(p^{m_i})!^{\text{grad } g_i/p^{m_i}} > p^{m_i}$ ist. Folglich muß jedes Polynom $g_i(X)$ separabel oder (rein) inseparabel und vom Grade 2 sein. Damit ist gezeigt, daß (i) gilt; aus $p^s = \prod_{i=1}^{l} p^{m_i}$ folgt nun auch sofort (ii).

Seien umgekehrt (i) und (ii) erfüllt. Dann folgt sofort

$u = \prod_{i=1}^{l} p^{m_i}$ und $\prod_{i=1}^{l} p^{m_i} = p^s$, also Rad(Z) = 0.

Der zweite Teil des Satzes folgt aus dem ersten, weil es dann keine inseparabeln Polynome mit $p^{m_i} = 2$ gibt.

Bemerkung 6.4

Das Polynom f ist separabel genau dann, wenn die im Beweis zu 6.2 angegebene Einschränkung von φ^* auf den Stabilisator $\{\sigma \in \mathfrak{S}_n : \sigma(\tilde{e}_1) = \tilde{e}_1\}$ des Idempotents $\tilde{e}_1$ ein Isomorphismus auf Gal(K:R) ist. Das ist nämlich genau dann der Fall, wenn $\ker \varphi^* \cap \mathfrak{S}_n = 1$ ist, welches nach Lemma 6.2 bedeutet, daß für alle i=1,...,l $e_i \cdot p^{m_i} = 1$ ist. Das ist aber genau dann der Fall, wenn f keine mehrfachen Nullstellen in K besitzt, also separabel ist.

Folgerung 6.5

Wenn Z(f,R) halbeinfach ist, gilt für die Ordnung der Galois-Gruppe von K über R $|\mathrm{Gal}(K:R)| = n!/k \cdot 2^r$, wo r die Anzahl der quadratisch-inseparabeln Faktoren in der Primfaktorzerlegung von f ist (d.h. also insbesondere r=0, falls char R $\neq$ 2).

Beweis: Wenn Z(f,R) halbeinfach ist, so ist nach Lemma 6.2 $\dim_R K = n!/k$ und nach Satz 6.3 $\dim_R K = 2^r \cdot \mathrm{Gal}(K:R)$.

Durch Kombination von 6.1 mit Folgerung 5.9 erhält man:

Folgerung 6.6

Wenn das Polynom f vom Grade $n \geqslant 5$ mehrfache Wurzeln in K besitzt, so gilt für die Anzahl k der Blockidempotenten von Z(f,R) $k \geqslant n$ oder k=1; im letzteren Fall ist f rein inseparabel.

Beweis: Nach Folgerung 5.9 kommt für $k < n$ nur k=1 und k=2 in Frage. Nun ist mit den Bezeichnungen in Lemma 6.2 $H := \ker\varphi^* \cap \overline{S}_n$ Normalteiler in $\overline{F}_1 = F_\varphi \cap \overline{S}_n$ und $H \neq 1$ nach Lemma 6.1, weil f mehrfache Wurzeln in K besitzt. Aus dem Beweis zu 5.9 sieht man, daß $\overline{F}_1 = \overline{S}_n$ genau für k=1 und $\overline{F}_1 = \overline{A}_n$ genau für k=2 gilt. Wegen $n \geqslant 5$ ist $\overline{S}_n \cong S_n$, und weil S_n nur den nichttrivialen Normalteiler A_n hat, ist $H = \overline{S}_n$ oder $H = \overline{A}_n$.

Nun gilt, wie man sich leicht überlegt, für beliebige positive natürliche Zahlen stets $a! \cdot b! \leqslant (a+b-1)!$. Wenn also $l \geqslant 2$ oder $\operatorname{grad} g_i > p^{m_i}$ für mindestens ein i ist, so gilt

$$H = \prod_{i=1}^{l} ((e_i \cdot p^{m_i})!)^{\operatorname{grad} g_i / p^{m_i}}$$

$$\leqslant (\sum_{i=1}^{l} e_i \cdot p^{m_i} \cdot \operatorname{grad} g_i / p^{m_i} - 1)!$$

$$= (n-1)! < (n-1)! \cdot n/2 = |\overline{A}_n|$$

d.h. $H \neq \overline{S}_n$ und $H \neq \overline{A}_n$.

Es muß also $l=1$ und $\operatorname{grad} g_1 = p^{m_1}$ sein. Das bedeutet aber, daß $|H| = n!$, also $H = \overline{S}_n$ ist und f nur eine Wurzel mit der Vielfachheit $e_1 \cdot p^{m_1} = n$ in K besitzt. Wegen $H \leqslant \overline{F}_1$ ist auch $\overline{F}_1 = \overline{S}_n$, also k=1.

Folgerung 6.7

Sei R ein endlicher Körper und f ein separables Polynom vom Grad $n \geq 4$. Die Anzahl k der Blockidempotenten von Z(f,R) ist stets $\geq n$.

Beweis: Mit der Bemerkung 6.4 ist $Gal(K:R) \cong \overline{F}_1$, wenn $\overline{F}_1$ der Stabilisator des Idempotents ε_1 in $\overline{S}_n$ ist. Aus dem Beweis von 5.9 folgt aber für $n \geq 4$ und $k < n$, daß $\overline{F}_1$ nicht kommutativ ist. Also muß $k \geq n$ sein.

Bemerkung 6.8

Wir zeigen mit einigen Beispielen, daß alle Fälle in Folgerung 5.9 auftreten können.

(a) Sei R der Körper der rationalen Zahlen. Das Polynom $f = X^5 - 3X + 3$ ist irreduzibel über R (nach dem Eisenstein-Kriterium) und hat genau drei reelle Wurzeln. Nach [8, chapter II, Th.8] ist die Galois-Gruppe Gal(K:R) die volle symmetrische Gruppe S_5. Nach Folgerung 6.5 ist also k=1.

(b) Sei R der Körper der rationalen Zahlen. Das Polynom $f = X^3 - 3X + 1$ ist irreduzibel über R (als rationale Nullstellen kämen nur 1 und -1 in Frage) und hat als Galois-Gruppe Gal(K:R) die alternierende Gruppe A_3 (vgl. [8, chapter II, Th.1]), weil die Diskriminante D(f) = 81 ein Quadrat in R ist. Nach 6.5 ist also k=2.

(c) Sei R der Körper der rationalen Zahlen. Das Polynom $f = X^4 - 2$ hat nach [11, chapter VIII, §2] als Galois-Gruppe eine Gruppe der Ordnung 8 (welche nach dem Beweis von 5.9 isomorph zu einer 2-Sylow-Gruppe in der symmetrischen Gruppe S_4 ist). Nach Folgerung 6.5 ist also k=3.

(d) Sei p eine Primzahl und R der Körper mit p Elementen. Die Galois-Gruppe des separabeln Polynoms $f = X^{p^n} - X$ hat die Ordnung n (vgl. [11,VII, §5]). Nach Folgerung 6.5 ist deshalb $k = (n-1)!$ (vgl. Bemerkung 5.10).

(e) Sei F ein Körper und $K:=F(X_1,\ldots,X_n)$ mit algebraisch unabhängigen Unbestimmten X_i. Die symmetrische Gruppe S_n operiert auf K durch Vertauschen der Unbestimmten. Sei U eine Untergruppe von S_n und $R:= K^U$ der Körper der U-invarianten Elemente von K. Das Polynom $f(X) = \prod_{i=1}^{n} (X - X_i)$ hat als Koeffizienten die symmetrischen Polynome s_i in den Unbestimmten X_j und ist daher in $R[X]$. Offensichtlich ist K der Zerfällungskörper des separabeln Polynoms f und U die Gruppe der Automorphismen von K über R. Nach Folgerung 6.5 ist $k = n!/|U|$.

LITERATURVERZEICHNIS

1. Auslander, M. und Goldman, O. : The Brauer group of a commutative ring. Trans. Amer. Math. Soc. 97 (1960), 1 - 24.

2. Azumaya, G. : On maximally central algebras. Nagoya Math. J. 2 (1951), 119 - 150.

3. DeMeyer, F. und Ingraham, E. : Separable algebras over commutative rings. Springer-Verlag Berlin/ Heidelberg/ New York 1971.

4. Dress, A. : Zur Theorie der Henselschen Ringe. Math. Zeit. 106 (1968), 355 - 360.

5. Greco, S. : Algebras over nonlocal Hensel rings. J. Algebra 8 (1968), 45 - 59.

6. Greco, S. : Algebras over nonlocal Hensel rings II. J. Algebra 13 (1969), 48 - 56.

7. Greco, S. : Henselization of a ring with respect to an ideal. Trans. Amer. Math. Soc. 144 (1969), 43 - 65.

8. Jacobson, N. : Lectures in abstract algebra, vol. III. Van Nostrand 1964.

9. Janusz, G. J. : Separable algebras over commutative rings. Trans. Amer. Math. Soc. 122 (1966), 461 - 479.

10. Kaplansky, I. : Fields and rings. The University of Chicago Press 1969.

11. Lafon, J. P. : Anneaux henséliens. Bull. Soc. Math. France 91 (1963), 77 - 107.

12. Lang, S. : Algebra. Addison-Wesley 1965.

13. Nagahara, T. : On separable polynomials over a commutative ring. Math. J. of Okayama Univ. 14 (1970), 175 - 181.

14. Nagahara, T. : On separable polynomials over a commutative ring II. Math. J. of Okayama Univ. 15 (1972), 149 - 162.

15. Nagata, M. : On the theory of henselian rings. Nagoya Math. J. 5 (1953), 45 - 57.

16. Nagata, M. : On the theory of henselian rings II. Nagoya Math. J. 7 (1954), 1 - 19.

17. Nagata, M. : Local rings. Interscience New York 1962.

18. Van der Waerden, B. L.: Algebra. Springer-Verlag Berlin/ Heidelberg/ New York 1967.

LEBENSLAUF

Ich bin am 27. April 1946 in Tübingen als erster von drei Söhnen geboren. Meine Eltern führten zu dieser Zeit einen sogenannten Tauschladen.

Mit dem Grundschulbesuch begann ich 1952 in Tübingen. Im Jahr darauf verlegten wir unseren Wohnsitz in das benachbarte Reutlingen, weil mein Vater dort als Rechtsanwalt tätig wurde.

1956 trat ich in das nächstgelegene altsprachliche Gymnasium, das Uhland-Gymnasium in Tübingen ein. Das Abitur legte ich im Frühjahr 1965 ab. Dann schloß sich eine zweijährige Dienstzeit als Soldat auf Zeit der Bundeswehr an wechselnden Standorten an.

Im Sommersemester 1967 begann ich mit dem Mathematikstudium an der Eberhard-Karls-Universität in Tübingen, wo ich im Frühjahr 1972 auch die Diplomprüfung in Mathematik bestand.

Ab Juni 1972 erhielt ich ein Promotionsstipendium nach dem Graduiertenförderungsgesetz. In dieser Zeit entstand unter der Anleitung von Herrn Professor Dr. G. Michler die vorliegende Arbeit "Die universelle Zerfällungsalgebra eines normierten Polynoms".

Seit dem 1. Oktober 1973 bin ich wissenschaftlicher Angestellter am Mathematischen Institut der Universität Gießen.

Meine akademische Ausbildung verdanke ich den Herren Professoren, Dozenten und Akademischen Räten G. Betsch, S. Breitsprecher, W. Gölz, H. Krüger, F. Lenz, G. Michler, H. Mitter, M. Reimer, H. Salzmann, H.H. Schaefer, W. Schulz, K. Strambach, O. Tamaschke, H. Wielandt, K. Zeller.

Chemoprint-Druck 63 Gießen Frankfurter Str. 129 Ruf (0641) 75712